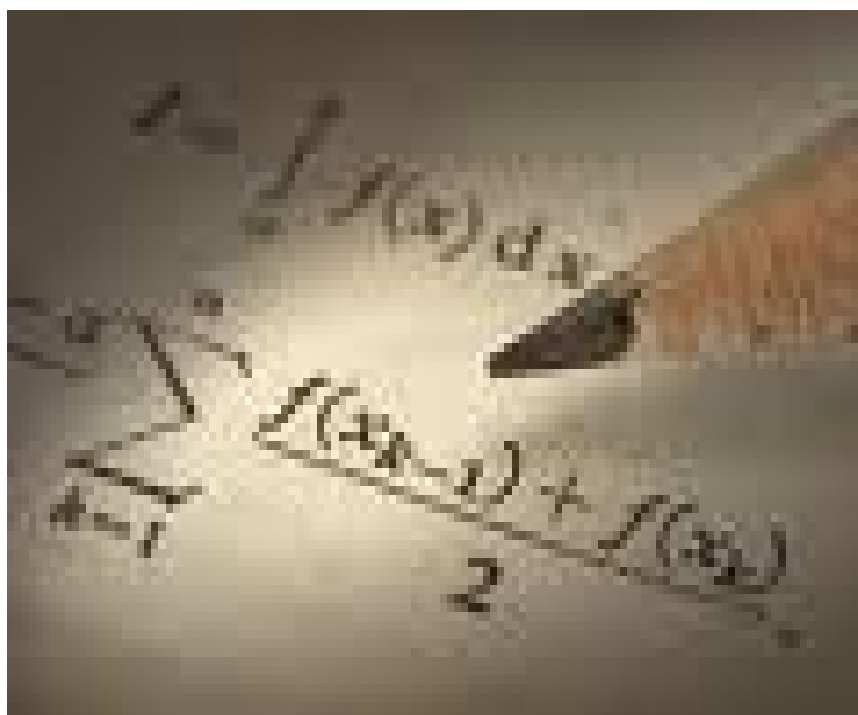


MATHEMATICA



Wprowadzenie do Teorii Liczb



I. Kompozycję i Partycję

Rozważmy problem dotyczący liczby sposobów w jaki liczba może być zapisana jako suma. Jeśli kolejność warunków w sumie jest brana pod uwagę, suma jest nazywana *kompozycją* a liczba kompozycji n jest oznaczana jako $c(n)$. Jeśli kolejność warunków nie jest brana pod uwagę suma jest *partycją* a liczba partycji n jest oznaczana przez $p(n)$. Zatem, kompozycja z 3 to

$$3 = 3; 3 = 1+2; 3 = 2+1; i 3 = 1 + 1 + 1;$$

tak więc $c(3) = 4$.

Partycja z 3 to

$$3 = 3; 3 = 2+1; i 3 = 1 + 1 + 1;$$

tak więc $p(3) = 3$

Istnieją trzy metody uzyskiwania wyników na kompozycje i partycje. Po pierwsze, przez czysto kombinatoryczne argumenty, po drugie przez argumenty algebraiczne z generowaniem serii i w końcu działania analityczne na wygenerowanej serii. Omówimy pierwsze z dwóch tych metod. Najpierw rozważmy kompozycję, ponieważ są łatwiejsze w obsłudze niż partycje. Funkcję $c(n)$ można łatwo określić w następujący sposób. Rozważmy n zapisane jako sumę jedynek. Mamy $n-1$ przestrzeni między nimi a w każdej przestrzeni możemy wstawić ukośnik, otrzymując 2^{n-1} możliwości odpowiadające 2^{n-1} kompozycji z n . Na przykład

$$3=1\ 1\ 1; 3 = 1=1\ 1; 3 = 1\ 1=1; 3 = 1=1=1$$

Zilustrujemy to metodą algebraiczną w tym raczej trywialnym przypadku jaki rozpatrujemy

$$\sum_{n=1}^{\infty} c(n)x^n$$

Łatwo zweryfikować, że

$$\begin{aligned} \sum_{n=1}^{\infty} c(n)x^n &= \sum_{m=1}^{\infty} (x + x^2 + x^3 + \dots)^m \\ &= \sum_{m=1}^{\infty} \left(\frac{x}{1-x} \right)^m = \frac{x}{1-2x} = \sum_{n=1}^{\infty} 2^{n-1} x^n \end{aligned}$$

Bardziej interesujące jest określenie liczby kompozycji $c^*(n)$ w części nieparzystej. Tu mamy podejście algebraiczne

$$\begin{aligned} \sum_{n=1}^{\infty} c^*(n)x^n &= \sum_{m=1}^{\infty} (x + x^3 + x^5 + \dots)^m \\ &= \sum_{m=1}^{\infty} \left(\frac{x}{1-x^2} \right)^m = \frac{x}{1-x-x^2} = \sum F(n)x^n \end{aligned}$$

Przez krzyżowe pomnożenie ostatnich dwóch wyrażeń zobaczymy ,że

$$F_{n+2} = F_n + F_{n+1}; F_0 = 1; F_1 = 1$$

Zatem F'y są to tak zwane liczby Fibonacciego

$$1; 1; 2; 3; 5; 8; 13; \dots$$

Funkcja generująca daje dwa wyraźne wyrażenia dla tych liczb. Pierwsze przez "częściowe frakcjonowanie" $x/(1-x-x^2)$, rozwijając każdy warunek jako szereg potęgowy i porównując współczynniki, uzyskujemy

$$F_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}$$

Inne wyrażenie dla F_n uzyskuje się przez zaobserwowanie ,że

$$\frac{x}{1-x-x^2} = x(1 + (x+x^2)^1 + (x+x^2)^2 + (x+x^2)^3 + \dots).$$

Porównując współczynniki uzyskamy

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \dots$$

Można rozważyć problem wnioskowania tej formuły poprzez argumenty kombinatoryczne.

Przypuśćmy ,że oznaczmy przez $a(n)$ liczbę kompozycji n ze wszystkich składników , co najwyżej 2, a przez $b(n)$ liczbę kompozycji z n ze wszystkimi składnikami, przynajmniej 2. Ciekawy wynik jest taki ,że $a(n) = b(n+2)$. Udowodnię ten wynik i zasugeruję problem znajdowania uzasadnionego uogólnienia.

Najpierw zwróć uwagę ,że $a(n) = a(n-1) + a(n-2)$. Wynika to z faktu ,że każda dopuszczalna kompozycja kończy się w 1 lub 2. Usuwając ten ostatni składnik, uzyskamy dopuszczalne kompozycje z $n-1$ i $n-2$, odpowiednio. Ponieważ $a(1) = 1$ a $a(2) = 2$, wynika stąd ,że $a(n) = F_n$. Funkcja $b(n)$ spełnia tą samą formułę rekurencyjną. Faktycznie, jeśli ostatni składnik w dopuszczalnej kompozycji z n to 2, usuwając go uzyskujemy dopuszczalną kompozycję z $n-2$; jeśli ostatni składnik jest większy niż 2, redukujemy go o 1 uzyskujemy dopuszczalną kompozycję z $n-1$. Ponieważ $b(2) = b(3) = 1$, wynika z tego ,że $b(n) = F_{n-2}$ więc $a(n) = F_n = b(n+2)$. Ciekawym pomysłem dla kompozycji jest waga kompozycji. Przypuśćmy ,że przydzieliliśmy każdej

kompozycji liczbę nazwaną wagą, która jest iloczynem składników. Określimy sumę wag $w(n)$ kompozycji z n . Funkcja generująca $w(n)$ to

$$\sum_{n=1}^{\infty} w(n)x^n = \sum_{m=1}^{\infty} (x + 2x^2 + 3x^3 + \dots)^m = \frac{x}{1 - 3x + x^2}$$

Z tego widzimy, że $w(n) = 3w(n-1) - w(n-2)$.

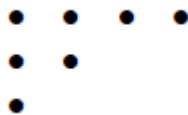
Wróćmy teraz do partycji. Nie ma prostej, jasnej formuły dla $p(n)$. Naszym głównym celem będzie udowodnienie formuły rekurencyjnej

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) + \dots$$

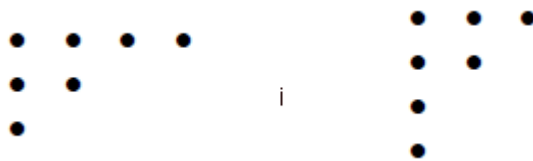
odkrytej przez Eulera. Algebraiczne podejście do teorii partycji zależy od manipulacji algebraicznych z funkcją generującą

$$\sum_{n=1}^{\infty} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)\dots}$$

i powiązanych funkcji dla ograniczenia partycji. Podejście kombinatoryczne zależy od zastosowania diagramu partycji Ferrera. Na przykład diagram partycji Ferrera dla $7 = 4 + 2 + 1$ wygląda tak



Użyteczne jest tu pojęcie sprzężenia partycji. Uzyskuje się to przez odzwierciedlenie na diagramie linii schodzącej z górnego lewego rogu pod kątem 45° . Na przykład partycje



są sprzężone jedna z drugą. Koresponduje to niemal natychmiast z poniższymi twierdzeniami:

Liczba partycji z n dzielona na m części jest równa liczbie partycji z n dzielonej na części, z której największą jest m

Liczba partycji z n dzielona na więcej niż m części jest równa liczbie partycji z n dzielonej na części nie przekraczające m

Nieco innej natury jest to : Liczba partycji z n dzielona na nieparzyste części jest równa liczbie partycji z n dzielonej na odrębne części. Podam do tego dowód algebraiczny. Skorzystamy raczej z oczywistych funkcji generujących dla wymaganych partycji, a wynik pokaże coś takiego

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\dots} = 1 + x^1 + x^2 + x^3 + \dots$$

Mnożenie krzyżowe daje wynik intuicyjny

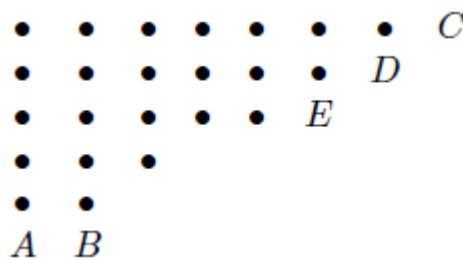
Teraz przejdziemy do ważniejszego twierdzenia ze względu na Eulera:

$$(1-x)(1-x^2)(1-x^3)\cdots = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots$$

gdzie wykładniki są liczbami w postaci $\frac{1}{2}k(3k \pm 1)$. Najpierw odnotujmy, że

$$(1-x)(1-x^2)(1-x^3)\cdots = \sum ((E(n) - O(n))x^n$$

gdzie $E(n)$ jest liczbą partycji z n dzieloną na parzystą liczbę odrębnych części a $O(n)$ liczbą partycji z n dzieloną na nieparzystą liczbę odrębnych części. Spróbujemy ustalić wzajemnie jednoznaczą zgodność między partycjami tych dwóch rozważanych rodzajów. Taka zgodność nie może być dokładna, gdyż taka dokładność prowadzi do stwierdzenia, że $E(n) = O(n)$. Weźmy wykres przedstawiający partycję z n dzieloną na dowolną liczbę nierównych części. Zaczniemy od niższej linii AB u dołu wykresu. Od C , najbardziej wysuniętego na północny wschód węzła rysujemy najdłuższą południowo-zachodnią linię dostępną na wykresie. Może ona zawierać tylko jeden węzeł. Linia CDE jest nazywana skrzydłem grafu



Zazwyczaj możemy przenieść bazę do pozycji w nowym skrzydle (równoległe i na prawo od "starego" skrzydła) Czasami możemy przeprowadzić operację odwrotną (przeniesienie skrzydła ponad bazę, poniżej starej bazy) Kiedy opisane działanie lub jej konwersja jest możliwa, prowadzi to z partycji z nieparzystą liczbą części do parzystej liczby części lub odwrotnie. Zatem, generalnie $E(n) = O(n)$. Jednak dwie sprawy wymagają specjalnej uwagi. Są one przedstawione na wykresach



W tych przypadkach n ma postać

$$k + (k + 1) + \cdots + (2k - 1) = \frac{1}{2}(3k^2 - k)$$

i

$$(k + 1) + (k + 2) + \cdots + (2k) = \frac{1}{2}(3k^2 + k)$$

W obu tych przypadkach jest ponad jedna partycja dzielona na parzystą liczbę części, lub jedna

dzielona na nieparzystą liczbę, w zależności czy k jest parzyste lub nieparzyste. Stąd $E(n) - O(n) = 0$, chyba że $n = \frac{1}{2}(3k \pm k)$, kiedy $E(n) - O(n) = (-1)^k$. Daje nam to twierdzenie Eulera

Teraz z

$$\sum p(n)x^n(1 - x - x^2 + x^5 + x^7 - x^{12} - \dots) = 1$$

otrzymujemy relację rekurencyjną dla $p(n)$, mianowicie

$$p(n) = p(n - 1) + p(n - 2) - p(n - 5) - p(n - 7) + p(n - 12) + \dots$$

II. Funkcje Arytmetyczne

Kolejnym tematem jakim się zajmiemy są funkcje arytmetyczne. Stanowią one główne obiekty zainteresowania w teorii liczb. Zajmiemy się teraz następującymi funkcjami

$$\pi(n) = \sum_{p \leq n} 1 \quad \text{Liczba liczb pierwszych nie przekraczających } n$$

$$\omega(n) = \sum_{p|n} 1 \quad \text{Liczba różnych liczb pierwszych stopnia } n$$

$$\Omega(n) = \sum_{p^i|n} 1 \quad \text{Liczba liczb pierwszych o współczynniku moc } n$$

$$\tau(n) = \sum_{d|n} 1 \quad \text{Liczba dzielników liczby } n$$

$$\sigma(n) = \sum_{d|n} d \quad \text{Suma dzielników liczby } n$$

$$\varphi(n) = \sum_{\substack{(a,n)=1 \\ 1 \leq a \leq n}} 1 \quad \text{Funkcja totient Eulera}$$

Funkcja Eulera (tocjent) zlicza liczbę liczb całkowitych $\leq n$ i względnie pierwszych dla n . Tu skupimy się szczególnie na funkcjach $\tau(n)$, $\sigma(n)$ i $\varphi(n)$. Mają one ważną właściwość, taką, że jeśli

$$n = ab \text{ and } (a; b) = 1$$

wtedy

$$f(ab) = f(a)f(b)$$

Dowolna funkcja spełniająca ten warunek jest nazywana słabo multiplikatywną lub po prostu multiplikatywną

Uogólnienie $\tau(n)$ i $\sigma(n)$ jest zapewnione przez

$$\sigma_k(n) = \sum_{d|n} d^k \quad \text{suma } k\text{-tych potęg dzielnika liczby } n$$

ponieważ $\sigma_0(n) = \tau(n)$ and $\sigma_1(n) = \sigma(n)$.

Funkcja φ również może być uogólniona w podobny sposób. Rozważymy to uogólnienie później ze względu na Jordana, $k(n)$ = liczba k -krotności $\leq n$ których g.c.d jest względnie pierwszą liczbą z n . Wyprowadzimy kilka elementarnych właściwości z nich i blisko powiązanych funkcji i określimy kilka specjalnych rozwiązanych i nierozwiązanych problemów związanych z nimi. Omówimy twierdzenie, która podaje jednolite podejście do tych funkcji i ujawnia nieoczekiwane połączenia między nimi. Później omówimy ważność tych funkcji. Funkcje $\omega(n)$, $\Omega(n)$, a w szczególności $\pi(n)$ są innej natury i zwrócimy na nie szczególną uwagę.

Przypuśćmy że mamy rozkład na czynniki potęgowe liczb pierwszych z n tak podane

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \quad \text{lub krócej} \quad n = \prod p^\alpha$$

Zauważ, że 1 nie jest liczbą pierwszą i uważamy za rzecz oczywistą dając się udowodnić, że niezależnie od celu, rozkład jest unikalny. W zakresie tym rozkład funkcji $\sigma_k(n)$ i $\varphi(n)$ są łatwe do określenia. Nie trudno zauważyć, że warunkami rozwinięcia iloczynu

$$\prod_{p|n} (1 + p^k + p^{2k} + \dots + p^{\alpha k})$$

są akurat dzielniki z n podniesione do potęgi k -tej. Stąd mamy pożądane rozwinięcie dla $\sigma_k(n)$. W szczególności

$$\tau(n) = \sigma_0(n) = \prod (\alpha + 1)$$

i

$$\sigma(n) = \sigma_1(n) = \prod_{p|n} (1 + p + p^2 + \dots + p^\alpha) = \prod_{p|n} \frac{p^{\alpha+1} - 1}{p - 1}$$

np. $60 = 2^2 * 3^1 * 5^1$.

$$\tau(60) = (2 + 1)(1 + 1)(1 + 1) = 3 \cdot 2 \cdot 2 = 12,$$

$$\sigma(60) = (1 + 2 + 2^2)(1 + 3)(1 + 5) = 7 \cdot 4 \cdot 6 = 168.$$

Wzory te ujawniają multiplikatywną naturę $\sigma_k(n)$. Dla uzyskania jasnego wzoru dla $\varphi(n)$ możemy skorzystać z dobrze znanych kombinatorycznej zasady

Zasada włączania i wyłączenia

Niech będzie dane N obiektów z których każdy może ale nie musi posiadać dowolne charakterystyki

A_1, A_2, \dots

niech $N(A_i, A_j, \dots)$ będzie liczbą obiektów mających charakterystyki A_i, A_j, \dots i możliwe inne wtedy liczba obiektów które nie mają żadnej z tych właściwości to

$$N - \sum N(A_i) + \sum_{i < j} N(A_i, A_j) - \sum_{i < j < k} N(A_i, A_j, A_k) + \dots$$

gdzie sumowanie rozciąga się na wszystkie kombinacje indeksów $1, 2, \dots, n$ w grupach po jeden, dwa, trzy itd i występują znaki warunków. Liczba całkowita będzie względnie pierwsza z n tylko jeśli nie jest podzielna przez żaden z czynników pierwszych z n . Niech A_1, A_2, \dots, A_s oznaczają podzielność przez p_1, p_2, \dots, p_s , odpowiednio. Wtedy zgodnie z zasadą kombinatoryki

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i < j} \frac{n}{p_i p_j} - \sum_{i < j < k} \frac{n}{p_i p_j p_k} + \dots$$

To wyrażenie może być rozłożone na czynnik do postaci

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

np.

$$\varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$$

Podobny argument pokazuje, że

$$\varphi_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right)$$

Wzór dla $\varphi(n)$ może być również zapisany w postaci

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

gdzie $\mu(d)$ pobiera wartości $0, 1, -1$. W rzeczywistości, $\mu(d) = 0$ jeśli d ma współczynnik kwadratowy, $\mu(1) = 1$ a $\mu(p_1 p_2 \dots p_s) = (-1)^s$. Funkcja ta odgrywa niespodziewanie istotną rolę w teorii liczb. Nasza definicja $\mu(n)$ ujawnia jej multiplikatywną naturę, ale nadal wydaje się raczej sztuczna. Ma jednak kilka bardzo ważnych właściwości które mogą być użyte jak definicje alternatywne. Udowodnimy najważniejszych z nich a mianowicie

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{jeśli } n = 1, \\ 0 & \text{jeśli } n \neq 1. \end{cases}$$

Ponieważ $\mu(d) = 0$ jeśli d zawiera współczynnik kwadratu, wystarczy aby podejrzewać, że n nie ma takiego współczynnika tj $n = p_1 p_2 \dots p_s$. Dla takiego $n > 1$

$$\sum_{d|n} \mu(d) = 1 - \binom{n}{1} + \binom{n}{2} - \dots = (1-1)^n = 0$$

Z definicji $\mu(1) = 1$ więc twierdzenie jest udowodnione

Jeśli suma tego wyniku ponad $n=1,2,\dots,x$ uzyskujemy

$$\sum_{d=1}^x \left\lfloor \frac{x}{d} \right\rfloor \mu(d) = 1$$

co jest inną definicją relacji

Inna ciekawą definicją właściwości jest to, że jeśli

$$M(x) = \sum_{d=1}^x \mu(d)$$

wtedy

$$\sum_{d=1}^x M\left(\left\lfloor \frac{x}{d} \right\rfloor\right) = 1$$

Jest to być może najbardziej elegancka definicja μ . Jeszcze jedną bardzo ważną właściwością jest to

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) = 1$$

Teraz zwrócimy uwagę na mnożenie i szereg Dirichleta. Rozważmy zbiór funkcji arytmetycznych. Mogą być połączone na różne sposoby dając nową funkcję. Na przykład, możemy zdefiniować $f + g$ przez

$$(f + g)(n) = f(n) + g(n)$$

i

$$(f * g)(n) = f(n) * g(n)$$

Mniej oczywistym trybem połączenia jest podanie $f \times g$ zdefiniowane przez

$$(f \times g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{dd'=n} f(d)g(d')$$

Może to być nazwane iloczynem dzielnika lub iloczynem Dirichleta. Motywacja dla tej definicji

jest taka Jeśli

$$F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}, \quad G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}, \quad ; \quad F(s) \cdot G(s) = \sum_{n=1}^{\infty} h(n)n^{-s},$$

wtedy łatwo jest stwierdzić, że $h = f \times g$. Zatem mnożenie Dirichleta funkcji arytmetycznych odpowiada zwykłemu mnożeniu odpowiednich szeregów Dirichleta:

$$f \times g = g \times f; (f \times g) \times h = f \times (g \times h)$$

tj. nasze mnożenie jest przemienne i łączne. Czysto arytmetyczny dowód tego wyniku jest łatwy do uzyskania. Zdefiniujmy teraz funkcję

$$e = e(n) : 1; 0; 0;$$

Łatwo zauważyć, że $f \times e = f$. Zatem funkcja e jest jednością w naszym mnożeniu. I trudno udowodnić, że jeśli $f(1) \neq 0$, wtedy f jest odwrotna w odniesieniu do e . Tak funkcja jest nazywana regularną. Zatem funkcje regularne tworzą grupy w odniesieniu do operacji \times . Innym twierdzeniem, którego dowód pominiemy, jest to, że iloczyn Dirichleta funkcji multiplikatywnej jest ponownie multiplikatywny. Wprowadzimy funkcję:

$$I_k : 1^k, 2^k, 3^k, \dots$$

Jest interesujące to, że zaczynając tylko do funkcji e i I_k , możemy zbudować wiele funkcji arytmetycznych i ich ważnych właściwości. Aby zacząć możemy zdefiniować $\mu(n)$ przez $\mu = I_0^{-1}$. Oznacza to oczywiście, że

$$\mu \times I_0 = e$$

$$\sum_{d|n} \mu(d) = \ell(n)$$

i możemy już zobaczyć, że jest to zdefiniowana właściwość funkcji μ . Możemy zdefiniować σ_k przez

$$\sigma_k = I_0 \times I_k.$$

Oznacza to, że

$$\sigma_k(n) = \sum_{d|n} d^k \cdot \ell(n),$$

co odpowiada naszej wcześniejszej definicji. Specjalne przypadki to

$$\tau = I_0 \times I_0 = I_0^2 \quad \text{i} \quad \sigma = I_1 \times I_1$$

Dalej możemy zdefiniować

$$\varphi_k = \mu \times I_k = I_0^{-1} \times I_k$$

Co oznacza, że

$$\varphi_k(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k$$

co znowu może być widziane jako odpowiednik naszej wcześniejszej funkcji. Specjalnym ciekawym przypadkiem jest tu

$$\varphi = \varphi_1 = \mu \times I_1.$$

Teraz aby uzyskać jakieś ważne relacje między naszymi funkcjami, odnotujmy tzw wzór inwersyjny Mobiusa. Z naszego punktu widzenia można powiedzieć ,ze

$$g = f \times I_0 \iff f = \mu \times g$$

Jest to oczywiście całkiem transparentne. Napiszmy w całości

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right)$$

W tej postaci jest znacznie mniej oczywista. Rozważmy teraz poniższą aplikację. Po pierwsze

$$\sigma_k = I_0 \times I_k \iff I_k = \mu \times \sigma_k$$

Oznacza to ,że

$$\sum_{d|n} \mu(d)\sigma_k\left(\frac{n}{d}\right) = n^k$$

Ważnym specjalnym przypadkiem są

$$\sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1.$$

i

$$\sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n.$$

Ponownie

$$\varphi_k = I_0^{-1} \times I_k \iff I_k = I_0 \times \varphi_k,$$

tak aby

$$\sum_{d|n} \varphi_k(d) = n^k.$$

Szczególnym przypadkiem szczególnego znaczenia będzie

$$\sum_{d|n} \varphi(n) = n.$$

Możemy uzyskać tożsamości w jakiś inny sposób. Zatem

$$\sigma_k \times \varphi_k = I_0 \times I_k \times I_0^{-1} \times I_k = I_k \times I_k$$

stąd

$$\sum_{d|n} \sigma_k(d) \varphi_k\left(\frac{n}{d}\right) = \sum_{d|n} d^k \left(\frac{n}{d}\right)^k = \sum_{d|n} n^k = \tau(n) n^k$$

Specjalny przypadkiem ciekawym jest

$$\sum_{d|n} \sigma(d) \varphi\left(\frac{n}{d}\right) = n \tau(n)$$

W celu zapewnienia naszym rachunkom zastosowanie do problemów związanych z dystrybucją liczb pierwszych, wprowadzamy jednoargumentowe działanie dla naszych funkcji nazwane różniczkowaniem

$$f'(n) = -f(n) \log n.$$

Motywacją dla tej definicji wynika z

$$\frac{d}{ds} \left(\sum \frac{f(n)}{n^s} \right) = - \sum \frac{\log n f(n)}{n^s}$$

Teraz określimy

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^\alpha \\ 0 & \text{if } n \neq p^\alpha \end{cases}$$

Łatwo zauważyć, że

$$\sum_{d|n} \Lambda(d) = \log n$$

W naszej notacji mnożenia Dirichleta mamy

$$\Lambda \times I_0 = -I'_0$$

tak aby

$$\Lambda = I_0^{-1} \times (-I'_0) = \mu \times (-I'_0)$$

lub

$$\Lambda(d) = - \sum_{d|n} \mu(d) \log \left(\frac{n}{d} \right) = \sum_{d|n} \mu(d) \log d$$

Przejdźmy teraz do interpretacji niektórych z naszych wyników w zakresie szeregu Dirichleta. Mamy odpowiednio

$$F(s) \longleftrightarrow f(n) \quad \text{jeśli} \quad F(s) = \sum \frac{f(n)}{n^s}$$

i wiemy, że mnożenie Dirichleta funkcji arytmetycznych odpowiada zwykłemu mnożeniu dla szeregu Dirichleta. Zaczniemy od

$$f \longleftrightarrow F, \quad 1 \longleftrightarrow 1, \quad \text{i} \quad I_0 \longleftrightarrow \zeta(s)$$

Co więcej

$$I_k \longleftrightarrow \sum_{n=1}^{\infty} \frac{n^k}{n^s} = \zeta(s - k)$$

również

$$\mu \longleftrightarrow \frac{1}{\zeta(s)} \quad \text{i} \quad I'_0 \longleftrightarrow \sum \frac{-\log n}{n^s} = \zeta'(s)$$

To daje

$$\sum \frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k)$$

Specjalne przypadki

$$\sum \frac{\tau(n)}{n^s} = \zeta^2(s)$$

i

$$\sum \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1)$$

Ponownie

$$\sum \frac{\varphi(n)}{n^s} = \frac{1}{\zeta(s)}$$

i

$$\sum \frac{\varphi_k(n)}{n^s} = \frac{\zeta(s-k)}{\zeta(s)}$$

ze specjalnym przypadkiem

$$\sum \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

Aby sprowadzić je do całkiem liczbowych wyników mamy

$$\begin{aligned} \sum \frac{\tau(n)}{n^2} &= \zeta^2(2) = \frac{\pi^4}{36}, \\ \sum \frac{\sigma_4(n)}{n^2} &= \zeta(2) \cdot \zeta(4) = \frac{\pi^2}{6} \cdot \frac{\pi^4}{90} = \frac{\pi^6}{540}, \\ \sum \frac{\mu(n)}{n^2} &= \frac{6}{\pi^2}. \end{aligned}$$

Co do naszej funkcji Λ , mamy

$$\Lambda = I_0^{-1} \times I_0'$$

co oznacza

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \frac{-\zeta'(s)}{\zeta(s)}$$

Twierdzenie o liczbach pierwszych zależy od wiarygodnego oszacowania dla

$$\Psi(x) = \sum_{n=1}^x \Lambda(n).$$

Rezerwywiście życzymy sobie pokazać, że $\Psi(x) \sim x$

Dowolny zarys całkowania po prawej stronie (*) wiąże się z koniecznością poznania gdzie znika $\zeta(s)$. Jest to jeden z centralnych problemów teorii liczb. Omówmy krótko szereg Dirichleta

Jeśli $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_a^{\alpha_s}$ definiujemy

$$\lambda(n) = (-1)^{\alpha_1 + \alpha_2 + \dots + \alpha_s}$$

Funkcja λ ma właściwości podobne do tych z funkcji μ . Darujemy sobie ćwiczenie aby pokazać, że

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{jeśli } n = r^2 \\ 0 & \text{jeśli } n \neq r^2 \end{cases}$$

Teraz

$$\zeta(2s) = \sum \frac{s(n)}{n^s} \quad \text{gdzie} \quad s(n) = \begin{cases} 1 & \text{jeśli } n = r^2 \\ 0 & \text{jeśli } n \neq r^2 \end{cases}$$

Stąd $\lambda \times I_0 = s$ tzn.

$$\sum \frac{\lambda(n)}{n^s} \cdot \zeta(s) = \zeta(2s)$$

lub

$$\sum \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}$$

Na przykład

$$\sum \frac{\lambda(n)}{n^2} = \frac{\pi^4}{90} / \frac{\pi^2}{6} = \frac{\pi^2}{15}$$

Rzucimy okiem na inny typ szeregu generującego mianowicie szeregu Lamberta . Szeregi są typu

$$\sum \frac{f(n)x^n}{1-x^n}$$

Łatwo wykazać ,że jeśli $F = f \times I_0$ wtedy

$$\sum \frac{f(n)x^n}{1-x^n} = \sum F(n)x^n$$

Ciekawy specjalny przypadki to

$$f = I_0, \quad \sum \frac{x^n}{1-x^n} = \sum \tau(n)x^n;$$

$$f = \mu, \quad \sum \mu(n) \frac{x^n}{1-x^n} = x;$$

$$f = \varphi, \quad \sum \varphi(n) \frac{x^n}{1-x^n} = \sum nx^n = \frac{x}{(1-x)^2}$$

Na przykład, biorąc $x=1/10$ w ostatnim równaniu, uzyskujemy

$$\frac{\varphi(1)}{9} + \frac{\varphi(2)}{99} + \frac{\varphi(3)}{999} + \dots = \frac{10}{81}$$

III. Rozkład liczb pierwszych

Najbardziej znanym dowodem we wszystkich "prawdziwych" matematykach jest dowód Euklidesa na istnienie nieskończenie wielu liczb pierwszych. Jeśli p było największą liczbą pierwszą, wtedy $(2*3*3 \dots p) + 1$ nie będzie podzielne przez żadną liczbę pierwszą do p a tym samym będzie to iloczyn liczb pierwszych powyżej p . Pomimo skrajnej prostoty dowód ten już budzi wiele skrajnych pytań np czy liczby $(2*3*3 \dots p) + 1$ są liczbami pierwszymi czy złożonymi? Znany jest brak ogólnego wyniku. Faktycznie, nie wiemy czy nieskończoność tych liczb jest pierwsza czy jest to nieskończoność złożona. Dowód można zmieniać na wiele sposobów. Zatem możemy rozważyć $(2*3*5 \dots p) - 1$ lub $p! + 1$ lub $p! - 1$. Znowu prawie nic nie wiadomo na temat takich czynników liczb. Ostatnie dwa zbiory liczb przywodzą na myśl problem który ujawnia jak w teorii liczb, może być

bardzo blisko najbardziej zawilego. Raczej banalne jest to, że dla $n > 2$, $n! - 1$ nie jest idealnym kwadratem. A co można powiedzieć o $n! + 1$? Cóż, $4! + 1 = 5^2$, $5! + 1 = 11^2$ a $7! + 1 = 71^2$. Jednak żadne inne przypadki nie są znane; ani nie wiadomo czy dowolna inna liczba $n! + 1$ jest idealnym kwadratem. Wrócimy do tego problemu przy równaniach diofantycznych. Po Euklidesie, kolejny znaczny postę w teorii rozkładu liczb pierwszych dokonał Euler.

Udowodnił, że $\sum \frac{1}{p}$ jest rozbieżny i opisał ten wynik przez powiedzenie, że liczb pierwszych jest więcej niż kwadratów. Chcę teraz przedstawić nowy dowód tego faktu – dowód, który w jakiś sposób jest powiązany z dowodem Euklidesa na istnienie nieskończenie wielu liczb pierwszych. Potrzebujemy najpierw (dobrze znanego) lematu w odniesieniu do podszeregu szeregu harmonicznego. Niech $p_1 < p_2 < \dots$ będzie sekwencją dodatnich liczb całkowitych i niech ich funkcja zliczająca będzie to

$$\pi(x) = \sum_{p \leq x} 1$$

Niech

$$R(x) = \sum_{p \leq x} \frac{1}{p}$$

Lemat: Jeśli $R(\infty)$ istnieje wtedy

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0.$$

Dowód

$$\pi(x) = 1(R(1) - R(0)) + 2((R(2) - R(1)) + \dots + x(R(x) - R(x - 1)))$$

lub

$$\frac{\pi(x)}{x} = R(x) - \left[\frac{R(0) + R(1) + \dots + R(x - 1)}{x} \right]$$

Ponieważ $R(x)$ zbliża się do granicy, wyrażenie wewnątrz nawiasów kwadratowych zbliża się do tej granicy i lemat jest udowodniony

W dalszej części zakładamy, że p są liczbami pierwszymi. Aby udowodnić, że $\sum \frac{1}{p}$ jest rozbieżny założymy przeciwieństwo tj $\sum \frac{1}{p}$ jest zbieżny (a stąd, że $\frac{\pi(x)}{x} \rightarrow 0$) i wynika sprzeczność..

W naszym założeniu istnieje n takie, że

$$\sum_{p > n} \frac{1}{p} < \frac{1}{2}$$

Ale teraz n jest ustalone jak że będzie również n takie, że

$$\frac{\pi(n!m)}{n!m} < \frac{1}{2n!}$$

Z takimi n i m tworzymy liczby m

$$T_1 = n! - 1, T_2 = 2n! - 1, \dots, T_m = mn! - 1$$

Zauważ, że żadne z T nie ma czynnika pierwszego $\leq n$ lub $\geq mn!$. Co więcej jeśli $p \mid T_i$ i $p \mid T_j$ wtedy $p \mid (T_i - T_j)$ tak, że $p \mid (i - j)$. Innymi słowy, wielokrotności p są p poza naszym zbiorem liczb. Stąd nie więcej niż $\frac{m}{p} + 1$ liczb podzielnych przez p . Ponieważ każda liczba ma przynajmniej jeden czynnik pierwszy mamy

$$\sum_{n < p < n!m} \left(\frac{m}{p} + 1 \right) \geq m$$

lub

$$\sum_{n < p} \frac{1}{p} + \frac{\pi(n!m)}{m} \geq 1.$$

Ale teraz (1) i (2) z prawej strony powinny być < 1 i mamy sprzeczność, która dowodzi naszego twierdzenia.

Dowód Eulera który jest bardziej istotny, zależy od jego bardzo ważnej tożsamości

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

Tożsamość ta jest zasadniczo analitycznym wyrażeniem twierdzenia o jednoznacznym rozkładzie na czynniki. Mamy

$$\begin{aligned} \prod_p \frac{1}{1 - \frac{1}{p^s}} &= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots \right) \\ &= \left(1 + \frac{1}{2^s} + \dots \right) \left(1 + \frac{1}{3^s} + \dots \right) \left(1 + \frac{1}{5^s} + \dots \right) \\ &= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots \end{aligned}$$

Euler twierdził, że dla $s=1$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \infty$$

tak więc

$$\prod_p \frac{1}{1 - \frac{1}{p}}$$

musi być nieskończone, co oznacza, że $\sum \frac{1}{p}$ musi być nieskończone. Ten argument, choć nie całkiem poprawny może z pewnością być ważny. W istocie można udowodnić bez większych trudności, że

$$\sum_{n \leq x} \frac{1}{n} - \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}$$

jest ograniczone.

Ponieważ $\sum_{n \leq x} \frac{1}{n} - \log x$ jest ograniczone, możemy, w sprawie logarytmów, uzyskać

$$\log \log x = \sum_{p \leq x} -\log \left(1 - \frac{1}{p}\right) + O(1)$$

tak więc

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + O(1)$$

Użyjemy tego wyniku później

Gauss i Legendre byli pierwszymi którzy podali rozsądne przybliżenie dla $\pi(x)$

Szczególnie przypuszczenie, że

$$\pi(x) \sim \frac{x}{\log x}$$

jest słynnym Twierdzeniem Liczb Pierwszych. Chociaż zostało to udowodnione w 1986 roku przez J.Hadamarda i de la Vallée Poussina, pierwsze znaczące postępy w tym kierunku poczynił Czebyszew. Uzyskał poniższe trzy główne wyniki;

- (1) Jest liczba pierwsza między n a $2n$ ($n > 1$)
- (2) Istnieją dodatnie stałe c_1 i c_2 takie, że

$$\frac{c_2 x}{\log x} < \pi(x) < \frac{c_1 x}{\log x}$$

- (3) Jeżeli $\frac{\pi(x)}{\log x}$ zbliża się do granicy, wtedy tą granicą jest 1

Udowodnimy że te trzy główne wyniki Czebyszewa używając jego metody zmodyfikowanej przez Landaua, Erdosa i w mniejszym stopniu L.Mosera

Wymagamy wielu lematów. Pierwsza z nich odnosi się do wielkości

$$n! \div \binom{2n}{n}$$

Jeśli chodzi o $n!$, możemy użyć przybliżenia Stirlinga

$$n! \sim n^n e^{-n} \sqrt{2\pi n}.$$

Jednak dla naszych celów wystarczy proste oszacowanie. Ponieważ

$$\frac{n^n}{n!}$$

jest tylko jednym z członów w rozwinięciu e^n ,

$$e^n > \frac{n^n}{n!}$$

i mamy następujący lemat

Lemat 1 $n^n e^{-n} < n! < n^n$

Ponieważ

$$(1+1)^{2n} = 1 + \binom{2n}{1} + \dots + \binom{2n}{n} + \dots + 1,$$

wynik stąd, że

$$\binom{2n}{n} < 2^{2n} = 4^n$$

Oszacowanie dla $\binom{2n}{n}$ nie jest tak surowe jak wygląda, ponieważ łatwo można to zauważyć ze wzoru Stirlinga

$$\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}$$

Korzystając z indukcji możemy pokazać, że

$$\binom{2n}{n} > \frac{4^n}{2n}$$

a zatem mamy

Lemat 2 $\frac{4^n}{2n} < \binom{2n}{n} < 4^n$

Zwróć uwagę, że $\binom{2n+1}{n}$ jest jednym z dwóch członów równania w wyrażeniu rozwinięcia $(1+1)^{2n+1}$.

Stąd też mamy

$$\text{Lemat 3} \quad \binom{2n+1}{n} < 4^n$$

Jako ćwiczenie możesz użyć tego dla udowodnienia, że jeśli

$$n = a + b + c + \dots$$

wtedy

$$\frac{n!}{a!b!c!\dots} < \frac{n^n}{a^a b^b c^c \dots}$$

Teraz możemy wywnioskować informacje w jaki sposób $n!$ i $\binom{2n}{n}$ są iloczynami liczb pierwszych. Przypuśćmy, że $e_p(n)$ jest wykładnikiem liczby pierwszej p w faktoryzacji potęgowej liczby pierwszej $n!$

$$n! = \prod p^{e_p(n)}$$

Łatwo udowodnić

$$\text{Lemat 4 (Legendre)} \quad e_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

W rzeczywistości $\left\lfloor \frac{n}{p} \right\rfloor$ jest liczbą wielokrotności p w $n!$, warunek $\left\lfloor \frac{n}{p^2} \right\rfloor$ dodaje dodatkowej wielokrotności p^2 itd np

$$e_3(30) = \left\lfloor \frac{30}{3} \right\rfloor + \left\lfloor \frac{30}{9} \right\rfloor + \left\lfloor \frac{30}{27} \right\rfloor + \dots = 10 + 3 + 1 = 14$$

Interesująca i czasami użytecznym wyrażeniem alternatywnym dla $e_p(n)$ jest podane

$$e_p(n) = \frac{n - s_p(n)}{p - 1}$$

gdzie $s_p(n)$ przedstawia sumę cyfr n kiedy n jest wyrażone na bazie p . Zatem o podstawie 3, 30 może być zapisane jako 1010 tak aby $e_3(30) = \frac{30-2}{2} = 14$ jak poprzednio

Teraz rozważmy złożenie $\binom{2n}{n}$ jako iloczyn liczb pierwszych. Niech $E_p(n)$ oznacza wykładnik p w $\binom{2n}{n}$ tj.

$$\binom{2n}{n} = \prod_p p^{E_p(n)}$$

Wyrażnie

$$E_p(n) = e_p(2n) - 2e_p(n) = \sum_i \left\{ \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right\}$$

Nasze alternatywne wyrażenia dla $e_p(n)$ dają

$$E_p(n) = \frac{2s_p(n) - s_p(2n)}{p-1}$$

W pierwszym wyrażeniu każdy warunek w sumie może łatwo być widziany jako 0 lub 1 i liczba warunków nie przekracza wykładnika najwyższej potęgi p która nie przekracza $2n$. Zatem

Lemat 5 $E_p(n) \leq \log_p(2n)$.

Lemat 6 Wkład p do $\binom{2n}{n}$ nie przekracza $2n$

Kolejne trzy lematy są natychmiastowe

Lemat 7 Każda liczba pierwsza w zakresie $n < p < 2n$ pojawia się dokładnie raz w $\binom{2n}{n}$

Lemat 8 Żadna liczba pierwsza w zakresie $\frac{2n}{3} < p < n$ nie jest dzielnikiem $\binom{2n}{n}$

Lemat 9 Żadna liczba pierwsza w zakresie $p > \sqrt{2n}$ nie pojawia się więcej niż raz w $\binom{2n}{n}$

Chociaż nie jest to konieczne w dalszej części, zabawnie jest zauważyć, że ponieważ

$$E_2(n) = 2s_2(n) - s_2(2n) \text{ i } s_2(n) = s_2(2n), \text{ mamy } E_2(n) = s_2(n)$$

Jako pierwsze zastosowanie tych lematów udowodnimy elegancki wynik

Twierdzenie 1 $\prod_{p \leq n} p < 4^n$.

Dowód jest przez indukcję. Zakładamy że twierdzenie jest prawdziwe dla liczb całkowitych $< n$ i zakładamy przypadki $n=2m$ i $n=2m+1$. Jeśli $n=2m$ wtedy

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} p < 4^{2m-1}$$

przez hipotezę indukcyjną. Jeśli $n=2m+1$ wtedy

$$\begin{aligned} \prod_{p \leq 2m+1} p &= \left(\prod_{p \leq m+1} p \right) \left(\prod_{m+1 < p < 2m+1} p \right) \\ &< 4^{m+1} \binom{2m+1}{m} \leq 4^{m+1} 4^m = 4^{2m+1} \end{aligned}$$

a indukcja jest skończona

Można wykazać przez głębszą metodę (Rosser), że

$$\prod_{p \leq n} p < (2.83)^n.$$

Właściwe twierdzenie liczb pierwszych jest równoważne

$$\sum_{p \leq n} \log p \sim n$$

Z Twierdzenia 1 można wywnioskować

Twierdzenie 2 $\pi(n) < \frac{cn}{\log n}$.

Wyrażnie

$$4^n > \prod_{p \leq n} p > \prod_{\sqrt{n} \leq p \leq n} p > \sqrt{n}^{\pi(n) - \pi(\sqrt{n})}$$

Biorąc logarytmy uzyskujemy

$$n \log 4 > (\pi(n) - \pi(\sqrt{n})) \frac{1}{2} \log n$$

lub

$$\pi(n) - \pi(\sqrt{n}) < \frac{n \cdot 4 \log 2}{\log n}$$

lub

$$\pi(n) < (4 \log 2) \frac{n}{\log n} + \sqrt{n} < \frac{cn}{\log n}.$$

Następnie udowodnimy

Twierdzenie 3 $\pi(n) > \frac{cn}{\log n}$

Do tego użyjemy Lematu 6 i 2 Z nich uzyskujemy

$$(2n)^{\pi(2n)} > \binom{2n}{n} > \frac{4^n}{2n}.$$

Biorąc logarytmy odkryjemy ,ze

$$(\pi(n) + 1) \log 2n > \log(2^{2n}) = 2n \log 2.$$

Zatem dla parzystego m

$$\pi(m) + 1 > \frac{m}{\log m} \log 2$$

i mamy wynik

Następnie uzyskamy szacunki dla $S(x) = \sum_{p \leq x} \frac{\log p}{p}$ Biorąc logarytm z $n! = \prod_p p^{e_p}$ odkrywamy ,że

$$n \log n > \log n! = \sum e_p(n) \log p > n(\log n - 1)$$

Czytelnik może uzasadnić ,że wprowadzono błąd zastępując $e_p(n)$ przez $\frac{n}{p}$ (oczywiście

$e_p(n) = \sum \left\lfloor \frac{n}{p^i} \right\rfloor$ jest na tyle małe, że

$$\sum_{p \leq n} \frac{n}{p} \log p = n \log n + O(n)$$

lub

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1)$$

Teraz można udowodnić

Twierdzenie 4 $R(x) = \sum_{p \leq x} \frac{1}{p} = \log \log x + O(1)$

Faktycznie

$$\begin{aligned} R(x) &= \sum_{n=2}^x \frac{S(n) - S(n-1)}{\log n} \\ &= \sum_{n=2}^x S(n) \left(\frac{1}{\log n} - \frac{1}{\log(n+1)} \right) + O(1) \\ &= \sum_{n=2}^x (\log n + O(1)) \frac{\log(1 + \frac{1}{n})}{(\log n) \log(n+1)} + O(1) \\ &= \sum_{n=2}^x \frac{1}{n \log n} + O(1) \\ &= \log \log x + O(1), \end{aligned}$$

zgodnie z życzeniem

Teraz zarys dowodu Czebszewa

Twierdzenie 5 *If $\pi(x) \sim \frac{cx}{\log x}$, then $c = 1$.*

Ponieważ

$$\begin{aligned} R(x) &= \sum_{n=1}^x \frac{\pi(n) - \pi(n-1)}{n} \\ &= \sum_{n=1}^x \frac{\pi(n)}{n^2} + O(1), \end{aligned}$$

$\pi(n) \sim \frac{cx}{\log x}$ oznaczałoby

$$\sum_{n=1}^x \frac{\pi(n)}{n^2} \sim c \log \log x.$$

Ale już wiemy, że $\pi(n) \sim \log \log x$ więc wynika, że $c = 1$

Teraz podamy dowód na postulat Bertranda.

Twierdzenie 6 Dla każdej liczby całkowitej r istnieje liczba pierwsza p taka

$$3 \cdot 2^{2r-1} < p < 3 \cdot 2^{2r}$$

Powtórzmy kilka naszych lematów w postaci w jakiej będą używane.

1. Jeśli $n < p < 2n$ wtedy p wystąpi dokładnie jeden raz w $\binom{2n}{n}$

2. Jeśli $2 \cdot 2^{2r-1} < p < 3 \cdot 2^{2r-1}$ wtedy p nie wystąpi w $\binom{3 \cdot 2^{2r}}{3 \cdot 2^{2r-1}}$

3. Jeśli $p > 2r+1$ wtedy p wystąpi przynajmniej raz w $\binom{3 \cdot 2^n}{3 \cdot 2^{n-1}}$.

4. Żadna liczba pierwsza nie wystąpi więcej niż $2r+1$ razy w $\binom{3 \cdot 2^{2r}}{3 \cdot 2^{2r-1}}$

Teraz porównamy $\binom{3 \cdot 2^{2r}}{3 \cdot 2^{2r-1}}$ i

$$\binom{2^{2r}}{2^{2r-1}} \binom{2^{2r-1}}{2^{2r-2}} \cdots \binom{2}{1} \left\{ \binom{2^{r+1}}{2^r} \binom{2^r}{2^{r-1}} \cdots \binom{2}{1} \right\}^{2r}$$

Zakładamy, że nie ma żadnej liczby pierwszej w zakresie $3 \cdot 2^{2r-1} < p < 3 \cdot 2^{2r}$. Wtedy, poprzez nasze lematy, odkryjemy, że każda liczba pierwsza, która występuje w pierwszym wyrażeniu również występuje w drugim z przynajmniej tak wysokimi krotnościami; to znaczy, drugie wyrażenie w niemniejszych niż w pierwszym. Z drugiej strony, obserwujemy, że dla $r \geq 6$

$$3 \cdot 2^{2r} > (2^{2r} + 2^{2r-1} + \cdots + 2) + 2r(2^{r+1} + 2^r + \cdots + 2),$$

i interpretacji $\binom{2n}{n}$ jako liczby sposobów wybrania n obiektów z $2n$, możemy stwierdzić, że drugie wyrażenie rzeczywiście jest mniejsze niż pierwsze. Ta sprzeczność dowodzi twierdzenia kiedy $r > 6$. Liczby pierwsze 7, 29, 97, 389 i 1543 pokazują, że twierdzenie jest również prawdziwe dla $r \leq 6$. Postulat Bertranda może być użyty do udowodnienia następujących wyników

1. $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ nigdy nie jest liczbą całkowitą
2. Każda liczba całkowita > 7 może być zapisana jako suma różnych liczb pierwszych
3. Każda liczba pierwsza p_n może być wyrażona w postaci

$$p_n = \pm 2 \pm 3 \pm 5 \pm \cdots \pm p_{n-1}$$

z błędem co najwyżej 1 (Scherk)

4. Równanie $\pi(n) = \varphi(n)$ ma dokładnie 8 rozwiązań

W 1949 roku sensacją okazało się odkrycie przez Erdosa i Selberga elementarnego dowodu Twierdzenia Liczb Pierwszych. Główny nowy wynik było następującym oszacowaniem, udowodnionym w elementarny sposób.

$$\sum_{p \leq x} \log^2 p + \sum_{pq \leq x} \log p \log q = 2x \log x + O(x)$$

Chociaż nierówność Selberga jest jeszcze daleka od Twierdzenia Liczb Pierwszych, może być później wyprowadzona z niej na różne sposoby bez uciekania się do dalszych wyników liczb teoretycznych. Podano kilka dowodów tego lematu, być może najprostszy jest Tauzawy i Iseki. Oryginalny dowód Selberga zależy od znaczenia funkcji.

$$\lambda_n = \lambda_{n,x} = \sum_{d|n} \mu(d) \log^2 \frac{x}{d}$$

I

$$T(x) = \sum_{n=1}^x \lambda_n x^n$$

Pięć lat później J.Lambek i L.Moser wykazali, że można udowodnić lemat Selberga w całkowicie elementarny sposób tj. Używając tylko właściwości liczb całkowitych. Jednym z głównych narzędzi dla zrobienia tego jest następująca racjonalna analogia z funkcją logarytmiczną. Niech

$$h(n) = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} \quad \text{a} \quad \ell_k(n) = h(kn) - h(k)$$

Udowodnimy w całkowicie elementarny sposób, że

$$|\ell_k(ab) - \ell_k(a) - \ell_k(b)| < \frac{1}{k}$$

Wyniki jakie ustaliliśmy są pożyteczne w badaniu wielkości funkcji arytmetycznych $\sigma_k(n)$, $\varphi_k(n)$ i $\omega_k(n)$. Ponieważ zależy to nie tylko od wielkości n ale również silnie od struktury arytmetycznej n nie możemy oczekiwać przybliżenia ich przez elementarne funkcje analityczne. Niemniej jednak będziemy widzieć, że "na podstawie średniej" te funkcje mają dość proste zachowanie. Jeśli f i g są funkcjami dla których

$$f(1) + f(2) + \dots + f(n) \sim g(1) + g(2) + \dots + g(n)$$

mówimy, że f i g mają tę "średnią kolejność" Zobaczmy, na przykład, że średnia kolejność $\tau(n)$ to $\log n$, że $\sigma(n)$ to $\frac{\pi^2}{6}n$ i że $\varphi(n)$ to $\frac{6}{\pi^2}n$. Rozważmy najpierw pierwszy heurystyczny argument

dla uzyskania średniej wartości $\sigma_k(n)$. Prawdopodobieństwo, że $r | n$ to $1/r$ i jeśli $r | n$ wtedy n/r wnosi $\left(\frac{n}{r}\right)^k$ dla $\sigma_k(n)$. Zatem oczekiwana wartość $\sigma_k(n)$ to

$$\begin{aligned} & \frac{1}{1} \left(\frac{n}{1}\right)^k + \frac{1}{2} \left(\frac{n}{2}\right)^k + \dots + \frac{1}{n} \left(\frac{n}{n}\right)^k \\ & = n^k \left(\frac{1}{1^{k+1}} + \frac{1}{2^{k+1}} + \dots + \frac{1}{n^{k+1}} \right) \end{aligned}$$

Dla $k = 0$ będzie to około $n \log n$. Dla $n \geq 1$ będzie to około $n^k \zeta(k+1)$, np dla $n = 1$ będzie to około

$$1 = \sum_{d=1}^x \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{n=1}^x M \left(\left\lfloor \frac{x}{n} \right\rfloor \right)$$

co poprzednio rozważaliśmy
Z

$$\sum_{d=1}^x \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = 1$$

mamy, po usunięciu nawiasów, pozwalających na błąd i podzieleniu przez x

$$\left| \sum_{d=1}^x \frac{\mu(d)}{d} \right| < 1$$

Właściwie to wiadomo, że

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d} = 0.$$

ale dowód na to jest równie głęboki jak na twierdzenie o liczbach pierwszych
Teraz rozważmy przypadek $f = 1$. Tu uzyskujemy

$$\sum_{n=1}^x \tau(n) = \sum_{n=1}^x \left\lfloor \frac{x}{n} \right\rfloor = x \log x + O(x)$$

W przypadku $f = I_k$ odnajdziemy, że

$$\sum_{n=1}^x \sigma_k(n) = \sum_{d=1}^x d^k \left\lfloor \frac{x}{d} \right\rfloor = \sum_{n=1}^x \left(1^k + 2^k + \dots + \left\lfloor \frac{x}{n} \right\rfloor^k \right)$$

W przypadku $f = \varphi$ przypomnijmy sobie, że $\sum_{d|n} \varphi(d) = n$, uzyskujemy

$$\frac{x(x+1)}{2} = \sum_{n=1}^x \sum_{d|n} \varphi(d) = \sum_{d=1}^x \left\lfloor \frac{x}{d} \right\rfloor \varphi(d) = \sum_{n=1}^x \Phi \left(\frac{x}{n} \right)$$

gdzie $\Phi(n) = \sum_{d=1}^n \varphi(d)$. Stąd łatwo uzyskamy

$$\sum_{d=1}^x \frac{\varphi(d)}{d} \geq \frac{x+1}{2}$$

z czego wynika, że średnio $\varphi(d) > \frac{d}{2}$.

Można również zastosować podobne odwrócenie kolejności sumowania aby uzyskać następujący

ważny drugi wzór inwersji Mobiusa

Twierdzenie

$$\text{If } G(x) = \sum_{n=1}^x F\left(\left\lfloor \frac{x}{n} \right\rfloor\right) \text{ then } F(x) = \sum_{n=1}^x \mu(n)G\left(\left\lfloor \frac{x}{n} \right\rfloor\right)$$

Dowód

$$\begin{aligned} \sum_{n=1}^x \mu(n)G\left(\left\lfloor \frac{x}{n} \right\rfloor\right) &= \sum_{n=1}^x \mu(n) \sum_{m=1}^{\lfloor x/n \rfloor} F\left(\left\lfloor \frac{x}{mn} \right\rfloor\right) \\ &= \sum_{k=1}^x F\left(\left\lfloor \frac{x}{k} \right\rfloor\right) \sum_{n|k} \mu(n) = F(x) \end{aligned}$$

Rozważmy ponownie nasze oszacowania

$$\tau(1) + \tau(2) + \dots + \tau(n) = n \log n + O(n).$$

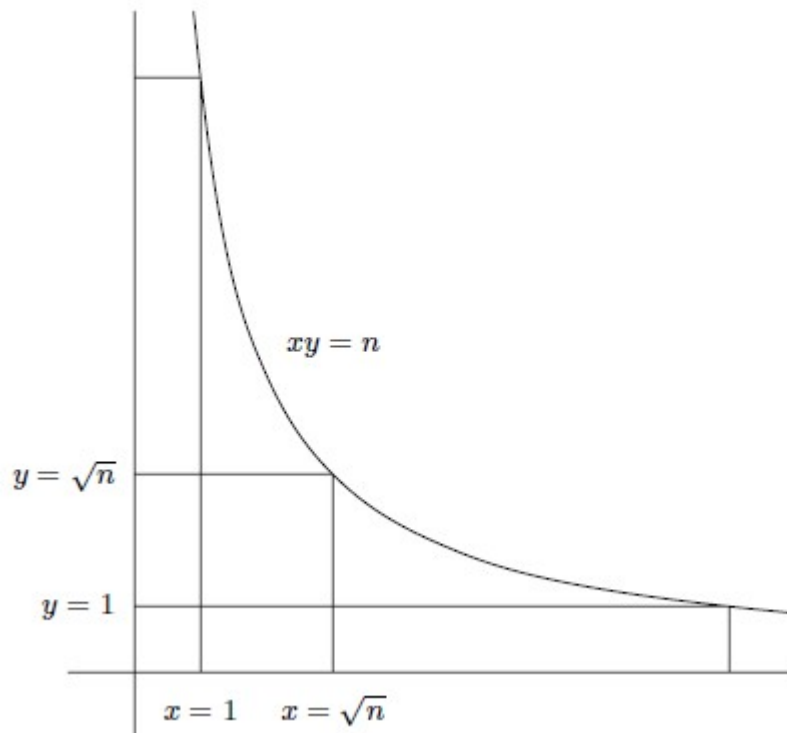
Pożyteczne jest uzyskanie geometrycznego wglądu w ten wynik. Oczywiście $\tau(r)$ jest liczbą punktów siatki na hiperboli $xy = r$, $x > 0$, $y > 0$. Również, każdy punkt siatki (x,y) , $x > 0$, $y > 0$, $xy \leq n$, leży na jakiejś hiperboli $xy=r$, $r \leq n$. Zatem

$$\sum_{r=1}^n \tau(r)$$

jest liczbą punktów siatki w regionie $xy \leq n$, $x > 0$, $y > 0$. Jeśli zsumujemy wzdłuż linii pionowych $x=1,2, \dots, n$ uzyskamy ponownie

$$\tau(1) + \tau(2) + \dots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \dots + \left\lfloor \frac{n}{n} \right\rfloor$$

W tym podejściu, symetria $xy = n$ o $x = y$ sugeruje jak poprawić to oszacowanie i uzyskać mniejszych błędów



Używając symetrii z powyższego rysunku, mamy, z $u = \lfloor \sqrt{n} \rfloor$ i

$$h(n) = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n},$$

$$\begin{aligned} \sum_{r=1}^n \tau(r) &= 2 \left(\left\lfloor \frac{n}{1} \right\rfloor + \dots + \left\lfloor \frac{n}{u} \right\rfloor \right) - u^2 \\ &= 2nh(u) - n + O(\sqrt{n}) \\ &= 2n \log \sqrt{u} + (2\gamma - 1)n + O(\sqrt{n}) \\ &= n \log n + (2\gamma - 1)n + O(\sqrt{n}). \end{aligned}$$

Przechodząc teraz do $\sum \sigma(r)$ mamy

$$\sigma(1) + \sigma(2) + \dots + \sigma(n) = 1 \left\lfloor \frac{n}{1} \right\rfloor + 2 \left\lfloor \frac{n}{2} \right\rfloor + \dots + n \left\lfloor \frac{n}{n} \right\rfloor$$

Aby uzyskać oszacowanie $\sum_{n=1}^x \sigma(n)$ ustawiamy $k = 1$ w tożsamości (uzyskanej wcześniej)

$$\sigma_k(1) + \sigma_k(2) + \dots + \sigma_k(x) = \sum_{n=1}^x \left(1^k + 2^k + \dots + \left\lfloor \frac{x}{n} \right\rfloor^k \right)$$

Mamy bezpośrednio

$$\begin{aligned}
\sigma(1) + \sigma(2) + \dots + \sigma(x) &= \frac{1}{2} \sum_{n=1}^x \left\lfloor \frac{x}{n} \right\rfloor \left\lfloor \frac{x}{n} + 1 \right\rfloor \\
&= \frac{1}{2} \sum_{n=1}^{\infty} \frac{x^2}{n^2} + O(x \log x) = \frac{x^2 \zeta(2)}{2} + O(x \log x) \\
&= \frac{\pi^2 x^2}{12} + O(x \log x).
\end{aligned}$$

Aby uzyskać podobne oszacowania dla $\varphi(n)$ zwróćmy uwagę że $\varphi(n)$ jest liczbą punktów siatki, które leżą na odcinku linii $x=r$, $0 < y < r$ i może być widoczna od początku. (Punkt (x,y) może być widoczny jeśli $(x,y) = 1$) Zatem $\varphi(1)+\varphi(2)+\dots+\varphi(n)$ jest liczbą widocznych punktów siatki w regionie z $n > x > y > 0$. Rozważmy dużo bardziej ogólny problem, mianowicie szacowanie liczby widocznych punktów siatki w większej klasie regionów. Za heurystyką przemawiają następujące argumenty. Punkt (x,y) jest niewidoczny z racji liczby pierwszej p jeśli $p \mid x$ i $p \mid y$. Prawdopodobieństwo, że to wystąpi to $1/p^2$. W związku z tym prawdopodobieństwo, że punkt jest niewidoczny to

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \dots\right)^{-1} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

Zatem liczba widocznych punktów siatki powinna być $6/\pi^2$ raza obszaru regionu/. W szczególności średni porządek $\varphi(n)$ powinien być około $6/\pi^2 n$. Teraz zarys dowodu na to, że w pewnych dużych regionach frakcji widocznych punktów siatki zawartych w regionie to w przybliżeniu $6/\pi^2$.

Niech R będzie regionem w płaszczyźnie mającej skończoną miarę Jordana i skończoną granicę. Niech tR oznacza region uzyskany przez powiększanie R radialnie przez t . Niech $M(tR)$ będzie obszarem tR , $L(tR)$ liczbą punktów siatki w tR a $V(tR)$ liczbą widocznych punktów siatki w tR . Jest intuicyjnie jasne, że

$$L(tR) = M(tR) + O(t) \quad \text{i} \quad M(tR) = t^2 M(R)$$

Stosując wzór do inwersji

$$L(tR) = V(tR) + V\left(\frac{t}{2}R\right) + V\left(\frac{t}{3}R\right) + \dots$$

okazuje się, że

$$\begin{aligned}
V(tR) &= \sum_{d=1} L\left(\frac{t}{d}R\right) \mu(d) = \sum_{d=1} M\left(\frac{t}{d}R\right) \mu(d) \\
&\approx M(tR) \sum_{d=1} \frac{\mu(d)}{d^2} \approx M(tR) \frac{6}{\pi^2} = t^2 M(R) \frac{6}{\pi^2}.
\end{aligned}$$

Przy $t = 1$ i R regionem $n > x > y > 0$, mamy

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) \approx \frac{n^2}{2} \cdot \frac{6}{\pi^2} = \frac{3}{\pi^2} n^2$$

Zwróć uwagę na szczegóły planu

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) = \frac{3}{\pi^2}n^2 + O(n \log n)$$

Wykazano (Chowla) ,że warunek błędu tu nie może być zredukowany do $O(n \log \log \log n)$. Walfitz pokazał ,że może być zastąpione przez $O(n \log^{\frac{3}{4}} n)$. Erdos i Shapiro wykazali ,że

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) - \frac{3}{\pi^2}n^2$$

zmienia się nieskończenie często. Później stworzymy aplikację naszego szacowania $\varphi(1) + \dots + \varphi(n)$ do teorii dystrybucji pozostałości kwadratowych. Nasz wynik może również być interpretowany mówiąc ,że jeśli para liczb całkowitych (a, b) są wybrane losowo a prawdopodobieństwo ,że będą one relatywnie pierwsze wynosi $6/\pi^2$. Na tym etapie stwierdzamy bez dowodu liczbę powiązanych wyników. Jeśli (a,b) są wybrane losowo oczekiwana wartość (a,b) to $\pi^2/6$. Jeśli $f(x)$ jest jedną z pewnych klas funkcji arytmetycznych, które zawierają x^α , $0 < \alpha < 1$,wtedy prawdopodobieństwo ,że $(x, f(x)) = 1$ to $6/\pi^2$, a wartość oczekiwana to $\pi^2/6$. To i powiązane wyniki zostały udowodnione przez Lambeka i Mosera. Prawdopodobieństwo ,że n liczb wybranych losowo jest relatywnie pierwszych to $\frac{1}{\zeta(n)}$.

Liczba $Q(n)$ liczb bez pierwiastków pod n to $\sim 6/\pi^2$, a liczba $Q_k(n)$ k-tej liczby bez potęgowej pod n to $\frac{n}{\zeta(k)}$

Pierwszy wynik pochodzi prawie bezpośrednio z

$$\sum Q\left(\frac{n^2}{r^2}\right) = n^2$$

tak ,że przez wzór na inwersję

$$Q(n^2) = \sum \mu(r) \left\lfloor \frac{n}{r} \right\rfloor^2 \sim n^2 \zeta(2)$$

Bardziej szczegółowy argument daje

$$Q(x) = \frac{6x}{\pi^2} + O(\sqrt{x})$$

Innym raczej zabawnym powiązaniem wynikiem , którego dowód zostawiam jako ćwiczenie, jest to ,że

$$\sum_{(a,b)=1} \frac{1}{a^2 b^2} = \frac{5}{2}$$

Wynik $Q(x)$ może być zapisany w postaci

$$\sum_{n=1}^x |\mu(n)| \sim \frac{6}{\pi^2} x$$

Można prosić o szacunki dla

$$\sum_{n=1}^x \mu(n) = M(x)$$

Rzeczywiście, wiadomo (ale trudno to udowodnić) że $M(x) = o(x)$. Zwróćmy uwagę na $\omega(n)$. Mamy

$$\omega(1) + \omega(2) + \dots + \omega(n) = \sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \sim n \log \log n$$

Zatem średnia wartość $\omega(n)$ to $\log \log n$.

To samo następuje w podobny sposób dla $\Omega(n)$. Stosunkowo niedawny rozwój w tym kierunku, ze względu na Erdosa, Kaca, Leveque, Tatumawę i innych jest liczba twierdzeń które są typowe.

Niech $A(x, \alpha, \beta)$ będzie liczbą liczb całkowitych $n \leq x$ dla których

$$\alpha \sqrt{\log \log n} + \log \log n < \omega(n) < \beta \sqrt{\log \log n} + \log \log n$$

Wtedy

$$\lim_{x \rightarrow \infty} \frac{A(x; \alpha, \beta)}{x} = \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-\frac{u^2}{2}} du$$

Zatem mamy przykład że $\omega(n) < \log \log n$ około pół raza. Można również udowodnić (Tatumawa) że podobny wynik otrzymamy dla $B(x, \alpha, \beta)$, liczba liczb całkowitych w zbiorze $f(1), f(2), \dots, f(x)$ jest wielomianem nierozkładalnym ze współczynnikiem całkowym dla którego $\omega(f(n))$ leży w zakresie podobnym do tych wyznaczonych dla $\omega(n)$. Inny typ wyniku, który ma zastosowanie jest następujący

Liczba $C(x, \alpha)$ liczb całkowitych $\leq x$ ma dzielnik pierwszy $> x^\alpha$, $1 > \alpha > \frac{1}{2}$. Jest $\sim -x \log \alpha$. Faktycznie mamy

$$\begin{aligned} C(x, \alpha) &= \sum_{x^\alpha < p < x} \frac{x}{p} \sim x \sum_{x^\alpha < p < x} \frac{1}{p} \\ &= x(\log \log x - \log \log \alpha) \\ &= x(\log \log x - \log \log x - \log \alpha) = -x \log \alpha. \end{aligned}$$

Na przykład gęstość liczb mających czynnik pierwszy przekraczający ich pierwiastek kwadratowy to $\log 2 \approx .7$.

Do tej pory rozważaliśmy głównie średnie zachowanie funkcji arytmetycznych. Możemy również zapytać o absolutne granice. Można udowodnić bez trudności że

$$1 > \frac{\varphi(n)\sigma(n)}{n^2} > \varepsilon > 0 \quad \text{dla wszystkich } n$$

Wiemy również że

$$n > \varphi(n) > \frac{cn}{\log \log n}$$

$$n < \sigma(n) < cn \log \log n$$

Jak dla $\tau(n)$, nie jest trudno wykazać, że

$$\tau(n) > (\log n)^k$$

nieskończenie często dla każdego k podczas gdy $\tau(n) < n^\varepsilon$ dla każdego ε i n wystarczająco dużych. Wskażemy ale nie udowodnimy głównego twierdzenie w tym kierunku

Jeśli $\varepsilon > 0$ wtedy

$$\tau(n) < 2^{(1+\varepsilon)\log n / \log \log n} \quad \text{dla wszystkich } n > n_0(\varepsilon)$$

podczas gdy

$$\tau(n) > 2^{(1-\varepsilon)\log n / \log \log n} \quad \text{nieskończenie często}$$

Nieco inny tryb problemu dotyczącego wartości średniej funkcji arytmetycznej był tematem pracy magisterskiej R. Trollope na Uniwersytecie Alberta parę lat temu.

Niech $s_r(n)$ będzie sumą cyfr n zapisywanych w bazie r . Mirski udowodnił, że

$$s_r(1) + s_r(2) + \dots + s_r(n) = \frac{r-1}{2} n \log_r n + O(n)$$

Trollope rozważał podobne sumy gdzie elementy po lewej uruchamiały pewne sekwencje takie jak liczby pierwsze, kwadraty itp.

Uzyskał on jeszcze inny zabawny wynik

$$\frac{s_1(n) + s_2(n) + \dots + s_n(n)}{n^2} \sim 1 - \frac{\pi^2}{12}$$

IV. Liczby niewymierne

Najlepiej znaną liczbą niewymierną jest $\sqrt{2}$. Zakładamy $\sqrt{2} \neq \frac{a}{b}$ z nowatorskim dowodem, który nie korzysta z podzielności argumentów.

Przypuśćmy, że $\sqrt{2} = a/b$ (a, b to liczby całkowite), z b tak małym jak to możliwe. Wtedy $b < a < 2b$ tak, że

$$\frac{2ab}{ab} = 2, \quad \frac{a^2}{b^2} = 2, \quad \text{ i } \quad \frac{2ab - a^2}{ab - b^2} = 2 = \frac{a(2b - a)}{b(a - b)}$$

Zatem

$$\sqrt{2} = \frac{2b - a}{a - b}$$

Ale $a < 2b$ i $a - b < b$; stąd mamy wymierną reprezentację $\sqrt{2}$ z mianownikiem mniejszym niż najmniejszy z możliwych!

Aby przekonać uczniów o istnieniu liczb niewymiernych, możesz zacząć od dowodu niewymierności $\log_{10} 2$. Jeśli $\log_{10} 2 = a/b$ wtedy $10^{a/b} = 2$ lub $10^a = 2^b$. Ale teraz lewa strona jest podzielna przez 5 podczas gdy prawa strona nie. Również nie tak znany jak powinien jest fakt, że $\cos 1^\circ$ (i $\sin 1^\circ$) jest niewymierny. Z

$$\cos 45^\circ + i \sin 45^\circ = (\cos 1^\circ + i \sin 1^\circ)^{45}$$

wniosujemy, że $\cos 45^\circ$ może być wyrażone jako wielomian całkowitych współczynników w $\cos 1^\circ$. Stąd jeśli $\cos 1^\circ$ był wymierny więc $\cos 45^\circ = 1/\sqrt{2}$

Fakt, że

$$\cos 1 = 1 - \frac{1}{2!} + \frac{1}{4!} - \dots$$

jest niewymierny może być udowodnione w ten sam sposób jak niewymierność e . W tym ostatnim przypadku, zakładamy wymierność e

$$\frac{b}{a} = e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{(a+1)!} + \frac{1}{(a+2)!} + \dots$$

co, po pomnożeniu przez $a!$, oznaczałoby, że $\frac{1}{a+1} + \frac{1}{(a+1)(a+2)} + \dots$ jest dodatnią liczbą całkowitą mniejszą niż 1.

Nieco bardziej skomplikowany argument może być użyty aby pokazać, że e nie jest niewymiernością kwadratową, tj. Jeśli a, b, c są liczbami całkowitymi wtedy $ae^2 + be + c \neq 0$. Jednak dowód na przestępną e jeszcze nie jest łatwy. Wcześniejsze edycje Hardy i Wright twierdzą że nie było łatwego dowodu, że π jest przestępna ale ta sytuacja została skorygowana w 1947 roku przez I. Nivena, który udowodnił niewymierność π co teraz przedstawimy

Niech

$$\pi = \frac{a}{b}, f(x) = \frac{x^n(a-bx)^n}{n!}, \quad \text{i} \quad F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \dots,$$

dodatnia liczba całkowita n będzie określona później. Ponieważ $n!f(x)$ ma współczynniki całkowite i wyrazy w x stopniach $\leq 2n$, $f(x)$ i wszystkie jej pochodne będą miały wartości całkowite przy $x = 0$. Również dla $x = \pi = a/b$. Ponieważ $f(x) = f(a/b-x)$. Z elementarnej analizy mamy

$$\frac{d}{dx}[F'(x) \sin x - F(x) \cos x] = F''(x) \sin x + F(x) \sin x = f(x) \sin x$$

Stąd

$$\int_0^\pi f(x) \sin x dx = [F'(x) \sin x - F(x) \cos x]_0^\pi = \text{liczba całkowita}$$

Jednak dla $0 < x < \pi$

$$0 < f(x) \sin x < \frac{n^n a^n}{n!} \rightarrow 0$$

dla dużych n . Stąd całka oznaczona jest dodatnia ale dowolnie mała dla dużych n ; ta sprzeczność pokazuje, że założenie $\pi = a/b$ jest nie do utrzymania. Ten dowód został rozszerzony na różne sposoby. Na przykład Niven również udowodnił, że kosinus liczby wymiernej jest niewymierny. Jeśli teraz π było wymierne, $\cos \pi = -1$ będzie niewymierne. Tą metodą można również udowodnić niewymierność pewnych liczb zdefiniowanych jako podstawa rozwiązań równań różniczkowych

drugiego stopnia spełniających specjalne warunki graniczne. Ostatnio podano wariacje dowodu Nivena, które choć bardziej złożone, unikają stosowania całek lub szeregu nieskończonego. Bardzo prostego dowodu, że π jest przestępne tj nie spełnia żadnego równania wielomianu o współczynnikach całkowitych wciąż brakuje. W odniesieniu do przestępności liczb istnieją zasadniczo trzy typy problemów: udowodnienie istnienia takich liczb, zbudowanie takiej liczby, i w końcu (dużo trudniejsze od dwóch pierwszych) udowodnienie, że pewne liczby które pojawiają się w analizie są przestępne. Przykładami liczb którym udowodniono przestępność są π , e , $e^{-\pi}$ i $\log 3 / \log 2$. Warte uwagi jest, że stałej Eulera γ i

$$\sum_{n=1}^{\infty} \frac{1}{n^{2s+1}} \quad (s \text{ jest liczbą całkowitą})$$

nie udowodniono niewymierności.

Dowód Cantora istnienia liczb przestępnych wychodził od pokazania, że liczby algebraiczne są policzalne podczas gdy liczby rzeczywiste nie. Zatem, każdy niepoliczalny zbiór liczb zawiera liczby przestępne. Na przykład jest liczba przestępna w postaci $e^{i\theta}$, $0 < \theta < \pi/2$, powiedzmy. Chociaż nie całkowicie odnosi się to do tematu, wykonamy teraz małą sztukę ze znikaniem używając liczby przestępnej $e^{i\theta}$ i konstrukcji Kuratowskiego.

Rozważmy następujący zbiór punktów na płaszczyźnie zespolonej. Zaczniemy od punktu O i niech S będzie zbiorem wszystkich punktów osiągalnych z niej przez szereg działań przesunięć jednostkowego punktu 1 w prawo i obrót ich o kąt θ o O . Jeśli oznaczymy takie przesunięcie i obrót przez T i R , odpowiednio, wtedy typowy punkt naszego zbioru S może być oznaczony $T^a R^b T^c \dots$. Następnie zaobserwujemy, że każdy punkt S musi mieć unikalną reprezentację w tej postaci. Rzeczywiście, T oznacza dodanie 1 do liczby zespolonej odpowiadającej temu punktowi a R oznacza mnożenie przez $e^{i\theta}$. Stąd wszystkie nasze punkty są wielomianami w $e^{i\theta}$ z dodatnimi współczynnikami, powiedzmy $z = P(e^{i\theta})$. Ale teraz jeśli punkt ma podwójną reprezentację, wtedy $P(e^{i\theta}) = R(e^{i\theta})$ i uzyskamy wielomian w $e^{i\theta}$ który neguje przestępny charakter $e^{i\theta}$. Niech $\sim T$ oznacza podzbiór S który składa się tych punktów S dla których ostatnie działanie konieczne do ich uzyskania to T i niech $\sim R$ oznacza podzbiór który składa się z punktów S dla których ostatnie działanie dla ich uzyskania to R . Wyraźnie $S = \sim T \cup \sim R$ a $\sim T \cap \sim R = \emptyset$. Przesunięcie S jednej jednostki w prawo wysła S do $\sim T$ tj czyni $\sim R$ niewidocznym! Z drugiej strony, obrót płaszczyzny przez \emptyset , wysła S do $\sim R$ czyniąc niewidocznym $\sim T$!

Do tej pory omówiliśmy tylko istnienie liczb przestępnych. Najłatwiejszym podejściem do rzeczywistej budowy takich liczb jest podejście przez twierdzenie Liouville'a.

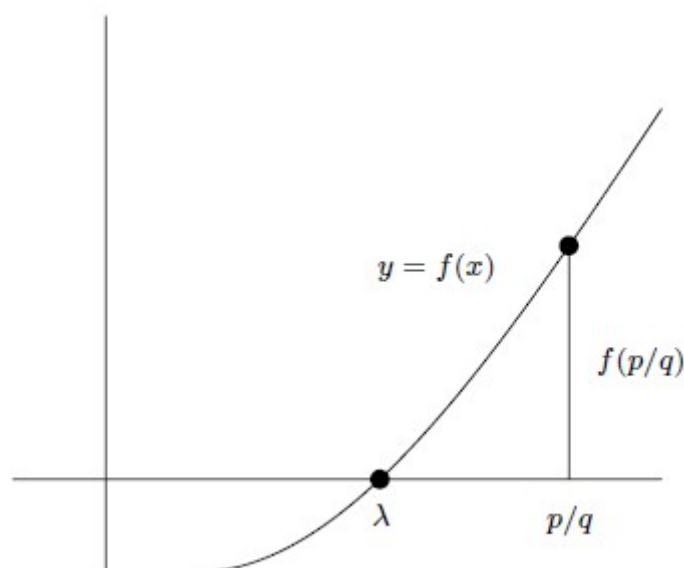
Mówimy, że liczba algebraiczna jest stopnia n jeśli spełnia równanie wielomianowe stopnia n . Mówimy, że liczba rzeczywista λ jest przybliżalna do porządku n pod warunkiem, że nierówność

$$\left| \lambda - \frac{a}{b} \right| < \frac{c}{b^n}$$

ma nieskończone rozwiązania dla jakiejś stałej c . Twierdzenie Liouville'a stanowi, że rzeczywista liczba algebraiczna stopnia n nie jest aproksymowalna do żadnego porządku większego niż n . Przypuśćmy, że λ jest stopnia n . Wtedy spełnia równanie

$$f(\lambda) = a_0 \lambda^n + a_1 \lambda^{n-1} + \dots + a_n = 0.$$

Jest liczba $M = M(\lambda)$ taka, że $|f'(x)| < M$ gdzie $\lambda - 1 < x < \lambda + 1$. Przypuśćmy teraz, że $p/q \neq \lambda$ jest aproksymacją do λ . Możemy założyć dość dobre przybliżenie aby zapewnić, że p/q leży w przedziale $(\lambda - 1, \lambda + 1)$



Rysunek 2

i jest bliżej λ niż dowolny inny pierwiastek $f(x) = 0$, tak więc $f(p/q) \neq 0$

Wyrażnie (Rysunek 2)

$$\left| f\left(\frac{p}{q}\right) \right| = \frac{1}{q^n} |a_0 p^n + a_1 p^{n-1} q + \dots + a_n q^n| \geq \frac{1}{q^n}$$

i

$$\left| \frac{f(p/q)}{\lambda - p/q} \right| < M$$

tak więc

$$\left| \lambda - \frac{p}{q} \right| > \frac{c}{q^n}$$

i twierdzenie jest udowodnione.

Chociaż twierdzenie Liouville'a wystarczy dla zbudowania wielu liczb przestępnych, można trochę uściślić. W szczególności pożądanym jest mieć twierdzenie następującego typu. Jeśli λ jest stopnia n wtedy

$$\left| \lambda - \frac{p}{q} \right| < \frac{M}{q^{f(n)}}$$

ma co najwyżej skończoną liczbę rozwiązań. Tu $f(n)$ może być wzięte jako n w twierdzeniu Liouville'a. Czy może być zmniejszone? Thue, około 1900 roku pierwszy wykazał, że można wziąć $f(n) = n/2$ a Siegel (1921) pokazał, że możemy przyjąć $f(n) = 2\sqrt{n}$. Znacząco poprawili to Dyson i Schneider na $\sqrt{2n}$. W 1955 roku F.K. Roth stworzył sensacyjny dowód, że możemy przyjąć $f(n) = 2 + \varepsilon$. Jego dowód jest długi i skomplikowany. To, że nie możemy przyjąć $f(n) = 2$ (zatem

wynik Rotha jest najlepszym z możliwych sposobów) można zobaczyć z następującego wyniku Dirichleta. Dla niewymiernego λ istnieje nieskończenie wiele rozwiązań

$$\left| \lambda - \frac{p}{q} \right| < \frac{1}{q^2}$$

Dowód nie jest trudny. Niech λ będzie niewymierna i rozważmy, dla stałego n , liczby $(\lambda), (2\lambda), \dots, (n\lambda)$, gdzie (x) oznacza "ułamkową część x ". Te n punktów jest różnymi punktami na $(0,1)$; stąd istnienie dwóch z nich powiedzmy $i\lambda$ i $j\lambda$ których odległość od siebie to $\leq 1/n$. Zatem mamy

$$(i\lambda) - (j\lambda) < \frac{1}{n}$$

lub

$$k\lambda - m \leq \frac{1}{n} \quad (k \text{ i } m \text{ liczby całkowite } \leq n)$$

i

$$\left| \lambda - \frac{m}{k} \right| \leq \frac{1}{nk} \leq \frac{1}{n^2}$$

co jest wymagane.

Teraz wrócimy do aplikacji z twierdzenia Liouville'a do budowania liczb przestępnych. Rozważmy

$$\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \dots + \frac{1}{10^{p!}} = \lambda_p$$

jak również liczbę rzeczywistą $\lambda = \lambda_\infty$. Łatwo jest sprawdzić, że

$$|\lambda_\infty - \lambda_p| < \frac{1}{\lambda^{n+1}}$$

dla każdego p . Stąd λ jest przybliżeniem do porządku n dla każdego n więc nie jest algebraiczna

V. Kongruencje

Tu będziemy rozwijać pewne aspekty teorii podzielności i kongruencji

Jeśli

$$a = \prod p^\alpha \quad ; \quad b = \prod p^\beta$$

wtedy łatwo zobaczyć, że

$$(a, b) = \prod p^{\min(\alpha, \beta)} \quad \text{podczas gdy} \quad [a, b] = \prod p^{\max(\alpha, \beta)}$$

Z tego łatwo wynika, że $(a, b) \cdot [a, b] = a \cdot b$. Pozostawmy to jako ćwiczenie wykazanie, że

$$(a, b) = \frac{1}{a} \sum_{\alpha=1}^{a-1} \sum_{\beta=1}^{a-1} e^{2\pi i \frac{\beta}{a} \alpha \beta}$$

Notacja $a \equiv b \pmod{m}$ dla $m \mid (a-b)$ spowodowana jest przez Gaussa. Dość oczywiste właściwości tej kongruencji to $a \equiv a$, $a \equiv b \Rightarrow b \equiv a$, i $a \equiv b$ i $b \equiv c \Rightarrow a \equiv c$, tzn. \equiv jest ekwiwalencją relacji. Łatwo jest również udowodnić, że $a \equiv b$ i $c \equiv d$ razem implikują $ac \equiv bd$; w szczególności $a \equiv b \Rightarrow ka \equiv kb$. Jednak ta konwersja nie jest prawdą w ogólności. Zatem $2 \times 3 = 4 \times 3 \pmod{6}$ nie implikuje $2 \equiv 4 \pmod{6}$. Jednak, jeśli $(k,m) = 1$ wtedy $ka \equiv kb$ implikuje $a \equiv b$. Inny ważny wynik jest następujący

Twierdzenie Jeśli $a_1, a_2, \dots, a_{\varphi(m)}$ tworzy kompletny system residuów mod m wtedy więc $aa_1, aa_2, \dots, aa_{\varphi(m)}$ pod warunkiem $(a,m) = 1$

Dowód. Mamy $\varphi(m)$ pozostałości. Jeśli dwie z nich są kongruentne $aa_i \equiv aa_j$, $a(a_i - a_j) \equiv 0$. Ale $(a, m) = 1$ więc $a_i \equiv a_j$.

Aplikacją tych idei jest ważne twierdzenie Eulera:

Twierdzenie Jeśli $(a, m) = 1$ wtedy $a^{\varphi(m)} \equiv 1 \pmod{m}$

Dowód. Ponieważ $a_1, a_2, \dots, a_{\varphi(m)}$ są kongruentne do $aa_1, aa_2, \dots, aa_{\varphi(m)}$ w pewnej kolejności, ich iloczyny są kongruentne. Stąd

$$a^{\varphi(m)} a_1 a_2 \cdots a_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)}$$

Specjalnym przypadkiem o podstawowym znaczeniu jest przypadek $m = p$ gdzie mamy

$$(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}.$$

Mnożąc przez a mamy dla wszystkich przypadków $a^p \equiv a \pmod{p}$. Inny dowód tego wyniku przechodzi przez indukcję na a ; mamy

$$(a + 1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + 1 \equiv a^p + a \pmod{p}.$$

Można również użyć twierdzenia wielomianu i rozważyć $(1+1+\dots+1)^p$.

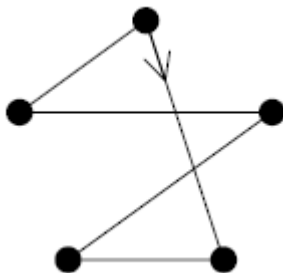
Jeszcze inny dowód mamy przez rozpatrywanie liczby regularnych wielokątów wypukłych gdzie każdy brzeg może być pokolorowany jednym z a kolorów. Liczba takich wielokątów to a^p , które to są monochromatyczne. Stąd $a^p - a$ nie jest monochromatyczne i te wchodzi do zbioru p każdy przez obrót przez $\frac{2\pi n}{p}$, $n = 1, 2, \dots, p-1$. Idea tego dowodu ma duże znaczenie i wrócimy do niego później.

Twierdzenia Fermata i Eulera mogą również być widziane z punktu widzenia grup teoretycznych. Liczby całkowite względnie pierwsze dla m i $< m$ formują grupę zgodnie z mnożeniem mod m . Najważniejszą rzeczą do sprawdzenia tu jest to, czy każdy element ma element odwrotny w systemie. Jeśli szukamy elementu odwrotnego dla a formujemy $aa_1, aa_2, \dots, aa_{\varphi(m)}$. Już widzieliśmy, że są to liczby $\varphi(m)$ niekongruentne mod m i względnie pierwsze dla m . Zatem, jedna z nich musi być jednostkowa i w następujący sposób mamy wynik. Teraz powrócimy do dowodu Eulera od Lagrange'a, który stanowi, że jeśli a jest elementem grupy G o porządku m , wtedy $a^m = 1$. W naszym przypadku oznacza to, że $a^{\varphi(m)} \equiv 1$ lub $a^{p-1} \equiv 1$ jeśli p jest liczbą pierwszą. Liczby całkowite pod p formują pole odnośnie $+$ i \times . Wiele z ważnych wyników teorii liczb jest opartych na fakcie, że część multiplikatywna tej grupy (zawierająca $p-1$ elementów) jest cykliczna tj. istnieje liczba g (nazwana pierwiastkiem pierwotnym z p) taka, że $1 = g^0, g^1, g^2, \dots, g^{p-1}$ są niekongruentne mod p . Fakt ten nie jest trywialny ale pominiemy ten dowód. Bardziej ogólny wynik grupy teoretycznej w którym zawarty jest określenie, że każde skończone pole jest automatycznie abelowe a grupa multiplikatywna jest cykliczna. W pierścieniu wielomianów ze współczynnikami posiada wiele twierdzeń elementarnej teorii równań. Na przykład jeśli $f(x)$ jest wielomianem którego elementy są resztami klas mod p wtedy $f(x) \equiv 0 \pmod{p}$ ma co najwyżej p rozwiązań. Dodatkowo jeśli r jest

pierwiastkiem wtedy $x - r$ jest dzielnikiem. Z drugiej strony, nie jest prawdą, że $f(x) \equiv 0 \pmod{p}$ ma przynajmniej jeden pierwiastek. Ponieważ $x^p - x \equiv 0$ ma co najwyżej p pierwiastków mamy rozkład na czynniki

$$x^p - x \equiv x(x - 1)(x - 2) \cdots (x - p + 1) \pmod{p}$$

Porównując współczynniki x mamy $(p-1)! \equiv -1 \pmod{p}$, co jest twierdzeniem Wilsona, Caley podał geometryczny dowód twierdzenia Wilsona. Rozważmy liczbę skierowanych wielokątów z wierzchołkami regularnego wielokątu (Rysunek 3)



Rysunek 3

To są $(p-1)!$ w liczbie których $p-1$ są regularne. Stąd nieregularne jedyńki to $(p-1)! - (p-1)$ w liczbie a te są w zbiorze p przez rotację.

Stąd

$$(p - 1)! - (p - 1) \equiv 0 \pmod{p}$$

i

$$(p - 1)! + 1 \equiv 0 \pmod{p}$$

Można również podać geometryczny dowód, który równocześnie daje twierdzenie Fermata i Wilsona i proponujemy jako problem znalezienie takiego dowodu. Twierdzenie Wilsona podaje konieczny i wystarczający warunek dla pierwszości: p jest liczbą pierwszą jeśli i tylko jeśli $(p-1)! \equiv -1$ ale jest to trudne praktyczne kryterium

Kongruencje z danymi pierwiastkami

Niech a_1, a_2, \dots, a_k będzie zbiorem różnych klas pozostałości \pmod{n} . Jeśli istnieje tam wielomian z całkowitymi współczynnikami takimi, że $f(x) \equiv 0 \pmod{n}$ ma pierwiastki a_1, a_2, \dots, a_k i żadnych innych, nazywamy to zbiorem kompatybilnym \pmod{n} . Niech liczba zbiorów kompatybilnych \pmod{n} będzie oznaczony $C(n)$. Ponieważ liczba podzbiorów tego zbioru składających z $0, 1, 2, \dots, n-1$ to 2^n , nazywamy $c(n) = \frac{C(n)}{2^n}$ współczynnikiem kompatybilności n . Jeśli $n = p$ jest liczbą pierwszą wtedy kongruencja

$$(x - a_1)(x - a_2) \cdots (x - a_k) \equiv 0 \pmod{n}$$

ma dokładnie pierwiastków a_1, a_2, \dots, a_n . Stąd $c(p) = 1$. Wykazano, że $c(4) = 1$ podczas gdy $c(n) < 1$ dla $n = 6, 8, 9, 10$. Udowodnimy, że $c(n) < 1$ dla każdej liczby złożonej $n \neq 4$. Możemy również udowodnić, że średnia wartość $c(n)$ jest zerem tj

$$\lim_{n \rightarrow \infty} \frac{1}{n} (c(1) + c(2) + \dots + c(n)) = 0.$$

Ponieważ $c(n) = 1$ dla $n = 1$ i $n = p$ rozważymy tylko przypadek gdzie n jest liczbą złożoną. Przypuśćmy wtedy, że unikalny rozkład na czynniki pierwsze n jest podany przez $p_1^{\alpha_1} p_2^{\alpha_2} \dots$ z

$$p_1^{\alpha_1} > p_2^{\alpha_2} > \dots$$

Rozważmy oddzielne przypadki

- (1) n ma więcej niż jeden dzielnik pierwszy i
- (2) $n = p^\alpha$, $\alpha > 1$.

W przypadku (1) możemy zapisać

$$n = a * b, (a,b) = 1, a > b > 1$$

Teraz pokażemy, że jeśli $f(a) \equiv f(b) \equiv 0$ wtedy $f(0) \equiv 0$

Dowód. Niech $f(x) = c_0 + c_1x + \dots + c_mx^m$. Wtedy

$$\begin{aligned} 0 &\equiv a f(b) \equiv a c_0 \pmod{n} & i \\ 0 &\equiv b f(a) \equiv b c_0 \pmod{n} \end{aligned}$$

Teraz ponieważ $(a,b) = 1$ istnieje r, s takie, że $ar + bs = 1$ tak więc $c_0(ar+bs) \equiv 0$ i $c_0 \equiv 0$

W przypadku (2) możemy zapisać

$$n = p^{\alpha-1} p$$

Pokażemy, że $f(p^{\alpha-1}) \equiv 0$ i $f(0) \equiv 0$ implikując $f(k p^{\alpha-1}) \equiv 0$, $k=2,3,\dots$

Dowód. Ponieważ $f(0) \equiv 0$ mamy $c_0 \equiv 0$,

$$\begin{aligned} f(x) &\equiv c_1 + c_2 x^2 + \dots + c_m x^m & i \\ f(p^{\alpha-1}) &\equiv c_1 p^{\alpha-1} \equiv 0 \pmod{p^\alpha}, \end{aligned}$$

tak więc $c_1 \equiv 0 \pmod{p}$. Ale teraz $f(k p^{\alpha-1}) \equiv$, co było wymagane

Względnie pierwsze sekwencje sformowane przez iteracje wielomianów (Lambek i Moser)

Bellman przedstawił następujący problem. Jeśli $p(x)$ jest nieredukowalnym wielomianem z całkowitymi współczynnikami a $p(x) > x$ dla $x > c$, udowadnia, że $\{p^n(c)\}$ nie może być liczbą pierwszą dla wszystkich dużych n . Nie proponujemy rozwiązania tego problemu ale chcemy przedstawić kilka uwag.

Jeśli $p(x)$ jest wielomianem z całkowitymi współczynnikami, wtedy jest k iteracji zdefiniowanych rekurencyjnie przez $p^0(x) = x$, $p^{k+1}(x) = p(p^k(x))$. Jeśli a i b są liczbami całkowitymi wtedy

$$p^k(a) \equiv p^k(b) \pmod{(a-b)}$$

W szczególności dla $a = p^n(c)$ i $b=0$ mamy $p^{k+n}(c) \equiv p^k(0) \pmod{p^n(c)}$

Stąd

$$(p^{k+n}(c), p^n(c)) = (p^k(0), p^n(c))$$

Stąd

$$(p^{k+n}(c), p^n(c)) = (p^k(0), p^n(c)).$$

Stąd

$$(p^{k+n}(c), p^n(c)) = (p^k(0), p^n(c)).$$

Będziemy nazywać sekwencję $\{a_n\}$, $n \geq 0$, względnie liczby pierwsze jeśli $(a_m, a_n) = 1$ dla wszystkich wartości m, n z $m \neq n$.

Twierdzenie 1 $\{p^n(c)\}$, $n \geq 0$ jest względnie liczby pierwsze jeśli i tylko jeśli $(p^k(0), p^n(c)) = 1$ dla wszystkich $k \geq 0, n \geq 0$

Z tego wynika bezpośrednio wynik Bellmana: Jeśli $p^k(0) = p(0) \neq 1$ dla $k \geq 1$ i jeśli $(a, p(0)) = 1$ implikuje $(p(a), p(0)) = 1$ wtedy $\{p^n(a)\}$, $n \geq a$ jest liczbą względnie pierwszą kiedy $(c, p(0)) = 1$

Teraz zbudujemy wszystkie wielomiany $p(x)$ dla których $\{p^n(c)\}$, $n \geq 0$ jest względna liczbą pierwszą dla wszystkich c . Zgodnie z Twierdzeniem 1, $\{p^k(0)\} = \pm 1$ dla wszystkich $k \geq 1$, łatwo jest zauważyć biorąc $n = k$ i $c = 0$. Ale wtedy $\{p^k(0)\}$ musi być jedną z następujących sześciu sekwencji

$$\begin{aligned} &1, 1, 1, \dots \\ &1, -1, 1, \dots \\ &1, -1, -1, \dots \\ &-1, 1, 1, \dots \\ &-1, 1, -1, \dots \\ &-1, -1, 1, \dots \end{aligned}$$

Łatwo jest zauważyć że ogólne rozwiązanie $p(x)$ (z całkowitymi współczynnikami) m równań

$$p(a_k) = a_{k+1}, \quad k = 0, 1, 2, \dots, m-1$$

jest uzyskiwane ze szczególnego rozwiązania $p_1(x)$ jak poniżej

$$p(x) = p_1(x) + (x - a_1)(x - a_2) \cdots (x - a_{k-1}) \cdot Q(x),$$

gdzie $Q(x)$ jest wielomianem z całkowitymi współczynnikami

Twierdzenie 2 $\{p^n(c)\}$, $n \geq 0$, jest względnie pierwsza dla wszystkich c jeśli i tylko jeśli $p(x)$ należy do jednej z sześciu klas wielomianów

$$\begin{aligned}
& 1 + x(x-1) \cdot Q(x) \\
& 1 - x - x^2 + x(x^2-1) \cdot Q(x) \\
& 1 - 2x^2 + x(x^2-1) \cdot Q(x) \\
& 2x^2 - 1 + x(x^2-1) \cdot Q(x) \\
& x^2 - x - 1 + x(x^2-1) \cdot Q(x) \\
& -1 + x(x+1) \cdot Q(x)
\end{aligned}$$

W sprawie dystrybucji reszt kwadratowych

Duży segment teorii liczb może być scharakteryzowany przez rozpatrywanie jej jako badanie pierwszej cyfry po prawej stronie liczb całkowitych. Zatem, liczba jest podzielna przez n jeśli jej pierwsza cyfra jest zerem kiedy liczba jest wyrażona w podstawie n. Dwie liczby są kongruentne (mod n) jeśli ich pierwsze cyfry są takie same w podstawie n. Teoria reszt kwadratowych jest związana z pierwszymi cyframi kwadratów. Szczególnie interesujący jest przypadek gdzie podstawa jest liczbą pierwszą i będziemy się ograniczać do tego przypadku.

Jeśli weźmiemy na przykład $p = 7$, wtedy z kongruencjami (mod 7) mamy $1^2 \equiv 1 \equiv 6^2$, $2^2 \equiv 4 \equiv 5^2$ i $3^2 \equiv 2 \equiv 4^2$ oczywiście $0^2 \equiv 0$. Zatem 1,2,4 są kwadratami a 3,5,6 są niekwadratami lub nie resztami. Jeśli a jest resztą z p zapiszemy

$$\left(\frac{a}{p}\right) = +1$$

podczas gdy jeśli a jest nieresztą zapiszemy

$$\left(\frac{a}{p}\right) = -1.$$

Z $p \mid c$ zapiszemy $\left(\frac{c}{p}\right) = 0$. Jest to notacja przez wzgląd na Legendrea. Dla $p = 7$ sekwencja

$$\left(\frac{a}{p}\right) \text{ jest zatem}$$

++-+--

Dla $p = 23$ okazuje się być

++++-+-+---+-----

Ta sytuacja jest klarowna jeśli przyjmiemy punkt widzenia grup teoretycznych Klasy pozostałości (mod p) tworzą pole, którego grupa multiplikatywna (zawierająca p-1) jest cykliczna. Jeśli g jest generatorem tej grupy wtedy elementy mogą być zapisane $g^1, g^2, \dots, g^{p-1} = 1$. Parzyste potęgi g są resztami kwadratowymi; formują one podgrupę indeksu dwóch. Nieparzyste potęgi g są nieresztami kwadratowymi. Z tego punktu widzenia jest to jasne.

$$\text{reszta} \times \text{reszta} = \text{reszta}, \text{reszta} \times \text{niereszta} = \text{niereszta}, \text{niereszta} \times \text{niereszta} = \text{reszta}$$

Dalsze $1/a$ przedstawia unikalną inwersję a (mod p) i będzie resztą lub nieresztą w zależności czy

samo a jest resztą lub nieresztą. Centralnym twierdzeniem w teorii reszt kwadratowych stanowiącym jedno z najważniejszych wyników teorii liczb jest Prawo Wzajemności Reszt Kwadratowych udowodnione przez Gaussa około 1800 roku. Stanowi, że

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Prowadzi to do algorytmu wartości decyzyjnej (p/q) . Ponad 50 dowodów tego prawa podano, wliczając w to dowody Zassenhausa i Lehmera. W pierwszym dowodzie Gaussa (podał ich siedem) użył lematu – który mówi nam, że był w stanie udowodnić ze znacznymi trudnościami. Dla $p \equiv 1 \pmod{4}$ najmniejsza niereszta p nie przekracza $2\sqrt{p} + 1$. Wyniki jakie chcemy omówić dzisiaj są w części poprawionymi wynikami a bardziej ogólne zajmują się rozkładem sekwencji znaków $+i -w$ (a/p) , $a = 1, 2, \dots, p-1$

W 1839 roku Dirichlet, jako produkt uboczny śledztwa odnośnie liczby klas form kwadratowych, określił następujące twierdzenie: Jeśli $p \equiv 3 \pmod{4}$ wtedy wśród liczb całkowitych $1, 2, \dots, p-1/2$, jest więcej reszt niż niereszt. Chociaż jest to elementarne wyrażenie o liczbach całkowitych, wszystkie opublikowane dowody wliczając to Chunga, Chowla, Whitmana, Carlitza i Mosera obejmują szereg Fouriera. Landau bardzo chciał mieć dowód elementarny. Chociaż nieco podobne wyniki podali Whitman i Carlitz, wynik Dirichleta okazał się wyizolowany. Zatem żaden podobny nieszablonowy wynik nie jest znany w innych zakresach. W 1896 Aladow, w 1898 von Sterneck i w 1906 Jacobsthal zadali pytanie ile razy pojawi się kombinacja $++$, $--$, $-+$ i $- -$. Wykazali, że każda z czterech możliwości pojawiała się, jak można było oczekiwać, z częstotliwością $1/4$. W 1951 roku Perron zadał pytanie ponownie i udowodnił, że podobne wyniki otrzyma się, jeśli zamiast kolejnych liczb całkowitych, rozważymy liczby całkowite oddzielone przez odległość d . J.B.Kelly udowodnił, wyniki taki, że z grubsza rzecz biorąc, wykazuje, że reszty i niereszty są charakteryzowane przez tą właściwość. Jacobstahl również uzyskał częściowy wynik dla przypadków 3 kolejnych reszt i nie reszt. Niech R_n i N_n będą liczbą bloków n kolejnych reszt i niereszt, odpowiednio. Można by przypuszczać, że $R_n \sim N_n \sim p/2^n$. Wśród tych którzy przyczynili się do tej kwestii byli Vandiver, Bennet, Dorge, Hopf, Davenport i A.Brauer. Być może najciekawszy wynik osiągnął A.Brauer. Wykazał, że dla $p > p_0(n)$, $R_n > 0$ i $N_n > 0$. Naszkicujemy część jego dowodu. Zależy on od bardzo ciekawego wyniku Van der Waerdena (1927). Dane są k, l , istnieje liczba całkowita $N = N(k, l)$ taka, że jeśli jeden oddziela liczby całkowite $1, 2, \dots, N$ na k klas w jakikolwiek sposób, przynajmniej jedna z tych klas będzie zawierała ciąg arytmetyczny o długości l . Jest wiele pytań bez odpowiedzi o tym twierdzeniu, do których wrócimy w dalszych częściach. Wracając do pracy Brauera, pokażemy że udowodnił, że wszystkie liczby pierwsze mają, powiedzmy 7 kolejnych reszt. Jeden rozdziela liczby $1, 2, \dots, p-1$ na 2 klasy, reszt i nie reszt. Jeśli p jest dość duże jedna z tych klas będzie zawierała, wedle twierdzenia Van der Waerdena, 49 wyrazów w ciągu arytmetycznym, powiedzmy

$$a, a+b, a+2b, \dots, a+48b$$

Teraz jeśli $a/b = c$ wtedy mamy 49 kolejnych liczb o tym samym kwadratowym charakterze, mianowicie

$$c, c+1, c+2, \dots, c+48$$

Jeśli są to reszty to kończymy. Jeśli nie reszty, wtedy przypuszczamy, że d jest najmniejszą nieresztą z p . Jeśli $d \geq 7$ kończymy, wtedy $1, 2, \dots, 7$ są kolejnymi nieresztami. Jeśli $d \leq 7$ rozważmy 7 niereszt $c, c+d, c+2d, c+6d$. Jeśli teraz dzielimy to przez nieresztę d uzyskamy 7 reszt

$$\frac{c}{d}, \frac{c}{d} + 1, \dots, \frac{c}{d} + 6$$

a wynik jest kompletny Dowód istnienia niereszt jest znacznie bardziej skomplikowana. Ponadto warto zauważyć, że istnieje blok taki jak $+-+ \dots$ który nie jest objęty tymi metodami.

Teraz wrócimy do zagadnienia podniesionego przez Gaussa. Co można powiedzieć o najmniejszej nie reszcie n_p liczby pierwszej? Ponieważ 1 jest resztą, odpowiednie pytanie o reszty to "jaka jest najmniejsza reszta pierwsza r_p z p ?" Te kwestie zostały zaatakowane w 1920 roku przez wielu matematyków takich jak Nagel, Schur, Polya, Zeitz, Landau, Vandiver, Brauer i Winogradow. Nagel na przykład, udowodnił, że dla $p \neq 7, 23$, $n_p < \sqrt{p}$. Polya i Schur udowodnili, że

$$\sum_{n=a}^b \left(\frac{n}{p}\right) < \sqrt{p} \log p.$$

Implikuje to to, że jestnie więcej niż $\sqrt{p} \log p$ kolejnych reszt lub niereszt i, że zakres dużo większy niż $\sqrt{p} \log p$ ma tyle reszt co nie reszt. Używając tego wyniku i pewnych twierdzeń na temat rozkładu liczb pierwszych, Winogradow udowodnił, że dla $p > p_0$,

$$n_p < p^{\frac{1}{2\sqrt{\epsilon}}} \log^2 p < p^{.303}$$

Sprawdzając dowód Winogradowa odkryliśmy, że w jego metodzie p_0 jest zbyt duże, powiedzmy $p_0 > 10^{10^{10}}$. Niemniej jednak, pomimo licznych prób ten wynik Winogradowa nie został znacznie

poprawiony

W 1938 roku Erdos i Ko wykazali, że istnienie małych niereszt było ściśle związane z nieistnieniem Algorytmu Euklidesa w polach kwadratowych. To pozwoliło Brauerowi, Hua i Minowi ponownie zbadać kwestię wyraźnych granic dla najmniejszej nie reszty. Brauer już w 1928 roku udowodnił liczbę takich wyników, typowe jest, że dla wszystkich $p \equiv 1 \pmod{8}$

$$n_p < (2p)^4 + 3(2p)^2 + 1$$

a Hua i Min udowodnili na przykład, że dla $p > e^{250}$,

$$n_p < (60\sqrt{p})^{.625}$$

Małe liczby pierwsze (poniżej 10,000,000) były rozpatrywane przez Benneta, Chatlanda, Brauera, Mosera i innych. Całkiem niedawno, nieudowodniona poszerzona hipoteza Riemmana została zastosowana do tych problemów przez Linnika, Chowla, Erdosa i Ankena. Zatem, na przykład Anken użył rozszerzonej hipotezy Riemmana do udowodnienia, że $n_p \neq O(\log^2 p)$. W przeciwnym kierunku, Pillai (1945) udowodnił, że $p \neq o(\log \log p)$. Korzystając z pierwszej hipotezy Riemmana a później kilku głębszych wyników Linnika o liczbach pierwszych w ciągu arytmetycznym, Friedlander i Chowla poprawili to na $n_p \neq o(\log p)$. Pojawiło się kilka wyników w nieco innym kierunku stworzonych przez Brauera, Nagela, Skolema, Redei'a i Kanolda. Metoda Redei'a jest szczególnie interesująca. Używa on analogii skończonej geometrii rzutowej do fundamentalnego twierdzenia Minkowskiego o ciałach wypukłych do udowodnienia, że dla $p \equiv 1 \pmod{4}$, przynajmniej $1/7$ z liczb do \sqrt{p} są resztami i przynajmniej $1/7$ jest nie resztami.

Rozważmy najpierw siatkę punktów w kwadracie o rozmiarze m . Poszukamy oszacowania dla $V(m)$, liczby widocznych punktów siatki w kwadracie. Wcześniej znaleźliśmy coś takiego

$$[m]^2 = V(m) + V\left(\frac{m}{2}\right) + \dots$$

a odwracanie przez wzór inwersji Mobiusa daje

$$V(m) = \sum_{d \geq 1} \mu(d) \left[\frac{m}{d} \right]^2$$

Tak jak wcześniej prowadzi to do asymptotycznego oszacowania

$$V(m) \sim \frac{6}{\pi^2} m^2$$

Możemy również uzyskać jednak wyraźne oszacowania dla $v(m)$. Rzeczywiście, z dokładnego wzoru dla $V(m)$ można wykazać że dla wszystkich m , $V(m) > .6m^2$. Teraz weźmy $m = \lfloor \sqrt{p} \rfloor$. Dla racjonalnie dużego p mamy $V(\lfloor \sqrt{p} \rfloor) > .59m^2$. Teraz z każdym widocznym punktem siatki (a,b) zwiążemy liczbę $a/b \pmod{p}$. Teraz pokażemy, że wyraźny widoczny punkt odpowiada wyrażnej liczby. Zatem, jeśli $a/b = c/d$ wtedy $ad = bc$. Ale $ad < p$ i $bc < p$. Stąd, $ad = bc$ i $a/b = c/d$. Jednak $(a,b) = (c,d) = 1$ tak więc $a = c$ i $b = d$.

Ponieważ mamy przynajmniej $.59$ wyraźnych liczb reprezentowanych przez ułamek a/b , $a < \sqrt{p}$, $b < \sqrt{p}$, przynajmniej $.09$ z nich będzie odpowiadało nie resztom. Jeśli R oznacza liczbę reszt $< \sqrt{p}$ a N liczbą nie reszt $< \sqrt{p}$, wtedy $R + N = \sqrt{p}$ a $2RN > .09p$. Rozwiązanie tej nierówności daje $R, N > .04\sqrt{p}$. Jest to słabszy wynik niż Nagela ale ma tę zaletę, że przechowuje liczby pierwsze $p \equiv 3 \pmod{4}$ jak również $p \equiv 1 \pmod{4}$. Zatem, wyjątkami okazują się tylko liczby pierwsze 7 i 23 . Dla liczb pierwszych $p \equiv 1 \pmod{4}$, -1 jest nie resztą i może być używane razem z powyższą metodą dla uzyskania mocniejszych wyników. Można również skorzystać z istniejących wielu nie reszt $< \sqrt{p}$ dla udowodnienia istnienia jednej małej nie reszty, ale wyniki uzyskiwane w ten sposób nie są tak mocne jak wyniki Winogradowa.

VI. Równania diofantyczne

Tom 2 "Historii Teorii Liczb" Dicksona zajmował się równaniami diofantycznymi. Jest to tak duże jak pozostałe dwie części razem. Jest zatem oczywiste, że nie zajmiemy się wszystkimi rzeczami związanymi z tym tematem. Skupimy naszą uwagę na pewnych problemach, które są interesujące choć nie mają kluczowego znaczenia. Jednym z takich problemów jest równanie diofantyczne $n! + 1 = x^2$ wspomniane wcześniej w tekście. Problem datuje się od 1885 roku kiedy H. Brocard przypuszczał, że jedynym rozwiązaniem są $4! + 1 = 5^2$, $5! + 1 = 11^2$ i $7! + 1 = 71^2$. Około 1895 roku, Ramanujan podał to samo przypuszczenie ale nie poczynił postępów w rozwiązaniu problemu. Około 1940 roku, problem pojawił się jako elementarny (!) problem w *Monthly*. Nie zaproponowano żadnego rozwiązania. Jednak w 1950 roku niepoprawne rozwiązanie zostało opublikowane i od tego czasu zostało dokonanych kilka wadliwych prób udowodnienia tego wyniku. Ponownie około 1950 roku ktoś podjął siłową próbę sprawdzenia przypuszczenia dla $n = 50$. Jednak już wcześniej w swojej książce o teorii liczb, Krajczik już udowodnił wyniki do 5000. Jak wiemy problem pozostał. Teraz podamy oznaczenie metody Krajczika. Przypuśćmy, że chcemy sprawdzić $100! + 1$. Pracując z $(\text{mod } 103)$ mamy

$$100!(-2)(-1) \equiv -1, \quad 100! + \frac{1}{2} \equiv 0, \quad 100! + 1 \equiv \frac{1}{2} \equiv 52$$

Jeśli teraz 52 jest nieresztą ze 103 osiągniemy nasz cel. W przeciwnym razie możemy przeprowadzić podobne obliczenia z innym $p > 100$, powiedzmy 107 . Zauważ, że $100! + 1 \equiv 0 \pmod{101}$ nie daje żadnej informacji. Wariacje tej metody mogą być użyte do eliminacji wielu liczb hurtowo i to jest to co zrobił Krajczik. Mamy teraz zarys dowodu, że

$$n! + 1 = x^8.$$

ma tylko skończoną liczbę rozwiązań. Dowód ten zależy od dwóch faktów na który nieokazały się udowodnione:

- (1) Każdy dzielnik nieparzystej liczby pierwszej x^2+1 jest w postaci $4n+1$
- (2) Jest mniej więcej tak wiele liczb pierwszych $4n+1$ co $4n+3$

Teraza $n!+1 = x^8$ daje $n! = x^8 - 1 = (x^4+1)(x^2+1)(x^2-1)$; prawy składnik liczb pierwszych $4k+1$ i $4k-1$ jest ten sam a po lewej wszystkie nieparzyste czynniki pierwsze z $(x^4+1)(x^2+1)$ tj o $(n!)^{3/4}$ iloczynu są w postaci $4n+1$.

Teraz przejdziemy do całkiem innego problemu. Czy równanie

$$1^n + 2^n + \dots + (m-1)^n = m^n$$

ma rozwiązania w liczbach całkowitych innych niż $1+2=3$? Tu mamy kilka bliskich rozwiązań:

$$\begin{aligned} 3^2 + 4^2 &= 5^2, \\ 3^3 + 4^3 + 5^3 &= 6^3, \\ 1^6 + 2^6 + 4^6 + 7^6 + 9^6 + 12^6 + 13^6 + 15^6 + 16^6 + 18^6 + 20^6 + 22^6 + 23^6 &= 28^6 \end{aligned}$$

Teraz mamy zarys dowodu, że jeśli jakieś rozwiązanie istnieje wtedy $m > 10^{1000000}$.

Liczba wyizolowanych równań wyrażonych sumą n-tych potęg liczb całkowitych jako n-tych potęg liczb całkowitych są znane od dawna. Niektóre przykłady

$$\begin{aligned} 3^3 + 4^3 + 5^3 &= 6^3 \\ \sum_{i=1}^{100} i^4 - 1^4 - 2^4 - 3^4 - 8^4 - 10^4 - 14^4 - 72^4 &= 212^4 \\ 1^6 + 2^6 + 4^6 + 5^6 + 6^6 + 7^6 + 9^6 + 12^6 + 13^6 + 15^6 + 16^6 \\ &+ 18^6 + 20^6 + 21^6 + 22^6 + 23^6 = 28^6. \end{aligned}$$

Z drugiej strony jedynym znanym rozwiązaniem w liczbach całkowitych dla równania w tytule, jest $1 + 2 = 3$. Erdos przypuszczał, że jest to jedyne rozwiązanie. Naszym celem jest pokazanie, że jeśli równanie ma rozwiązanie z $n > 1$ wtedy $m > 10^{1000000}$.

Niech $S_n(m)$ oznacza $\sum_{i=1}^{m-1} i^n$. W dalszej części zakładamy

$$S_n(m) \equiv m^n, \quad n > 1$$

Możliwe jest zbadanie tego z różnymi modułami i tym samym uzyskać ograniczenia na m i n . Jest to w zasadzie nasza metoda, ale moduły są tak dobrane, że możemy połączyć wyniki kongruencji tak aby uzyskać bardzo duże granice dla m bez żmudnych obliczeń. Użyjemy poniższego lematu.

Lemat 1 Jeśli p jest liczbą pierwszą a $\varepsilon_n(p)$ jest zdefiniowane przez $\varepsilon_n(p) = -1$ kiedy $(p-1) \mid n$ a $\varepsilon_n(p) = 0$ kiedy $(p-1)$ nie jest podzielne przez n wtedy

$$S_n(p) \equiv \varepsilon_n(p) \pmod{p}$$

Przypuśćmy teraz $p \mid (m-1)$, wtedy

$$S_n(m) = \sum_{i=0}^{\frac{m-1}{p}-1} \sum_{j=1}^p (j+ip)^n \equiv \frac{m-1}{p} \cdot \varepsilon_n(p) \pmod{p}$$

Z drugiej strony $m \equiv 1 \pmod{p}$ tak więc przez

$$\frac{m-1}{p} \cdot \varepsilon_n(p) \equiv 1 \pmod{p}$$

Stąd $\varepsilon_n(p) \not\equiv 0 \pmod{p}$ tak więc z definicji $\varepsilon_n(p)$ wynika, że $\varepsilon_n(p) = -1$ a

$$p \mid (m-1) \text{ implikuje } (p-1) \mid n$$

Zatem można przedstawić następującą formę

$$\frac{m-1}{p} + 1 \equiv 0 \pmod{p}$$

lub

$$m-1+p \equiv 0 \pmod{p^2}$$

Z powyższego wynika, że $m-1$ jest wolnym kwadratem. Dalej, ponieważ łatwo jest sprawdzić, że $m-1 \neq 2$ wynika że $m-1$ musi mieć przynajmniej jeden pierwszy dzielnik, więc n jest parzyste. Teraz pomnożymy razem wszystkie kongruencje, która jest jedną dla każdego pierwszego dzielenia $m-1$. Ponieważ $m-1$ jest wolnym kwadratem, moduł wynikowy to $m-1$. Ponadto, iloczyny zawierające dwa lub więcej różnych współczynników postaci $(m-1)/p$ będą podzielne przez $m-1$. Zatem uzyskujemy

$$(m-1) \sum_{p \mid (m-1)} \frac{1}{p} + 1 \equiv 0 \pmod{m-1}$$

lub

$$\sum_{p \mid (m-1)} \frac{1}{p} + \frac{1}{m-1} \equiv 0 \pmod{1}$$

Jedynie wartości $m \leq 1000$ które spełniają powyższe to 3,7,43. Przejdziemy do opracowania trzech kongruencji, podobnych do powyższej, co w połączeniu z nią prowadzi do głównego wyniku. Równanie

$$S_n(m) \equiv m^n, \quad n > 1$$

może być zapisane w postaci

$$S_n(m+2) = 2m^n + (m+1)^n.$$

Przypuśćmy, że $p \mid (m+1)$. Używając

$$S_n(p) \equiv \varepsilon_n(p) \pmod{p}$$

i faktu, że n jest parzyste, uzyskujemy

$$p \mid (m+1) \text{ implikuje } (p-1) \mid n$$

i

$$\frac{m+1}{p} + 2 \equiv 0 \pmod{p}.$$

Z tego wynika, że żadna nieparzysta liczba pierwsza pojawia się z wykładnikiem większym niż jeden w $m+1$. Liczba pierwsza 2 jednak., wymaga specjalnej uwagi. Jeśli zbadamy

$$S_n(m) \equiv m^n, \quad n > 1$$

z modulo 4, i użyjemy faktu, że n jest parzyste, wtedy odkryjemy, że $m+1 \equiv 1$ lub $4 \pmod{8}$. Zatem $m+1$ jest nieparzyste lub zawiera dokładnie 2 do drugiej potęgi. Jeśli założymy drugą z możliwości wtedy można wstawić postać

$$\frac{m+1}{2p} + 1 \equiv 0 \pmod{p}.$$

Mnożymy wszystkie razem kongruencje powyższego typu. Ten moduł wtedy staje się $m+1/2$. Ponadto każdy warunek zawierający dwa lub więcej różnych współczynników $m+1/2p$ będą podzielne przez $m+1/p$ tak więc w uproszczeniu uzyskamy

$$\sum_{p \mid (m+1)} \frac{1}{p} + \frac{2}{m+1} \equiv 0 \pmod{1}$$

Przejdziemy do znajdowania dwóch lub więcej kongruencji podobnych do powyższej bez używania założenia, że $m+1$ równa się siedem. Przypuśćmy, że $p \mid 2m-1$ i niech $t = \frac{1}{2} \left(\frac{2m-1}{p} - 1 \right)$. Wyrażnie t jest liczbą całkowitą a $m-1 = tp + \frac{p-1}{2}$. Ponieważ n jest parzyste $a^n = (-a)^n$ tak, że

$$S_n\left(\frac{p-1}{2}\right) \equiv \frac{\varepsilon_n(p)}{2} \pmod{p}.$$

Teraz

$$S_n(m) = \sum_{i=0}^{t-1} \sum_{j=1}^{p-1} (j+ip)^n + \sum_{i=1}^{(p-1)/2} i^n \equiv \left(t + \frac{1}{2}\right) \varepsilon_n(p) \pmod{p}$$

Z drugiej strony $m^n \equiv 0 \pmod{0}$ tak więc

$$S_n(m) \equiv m^n, \quad n > 1 \quad i$$

$$S_n(m) = \sum_{i=0}^{t-1} \sum_{j=1}^{p-1} (j+ip)^n + \sum_{i=1}^{(p-1)/2} i^n \equiv \left(t + \frac{1}{2}\right) \varepsilon_n(p) \pmod{p}$$

implikują $\varepsilon_n(p) \neq 0$. Stąd $p-1/n$ i z twierdzenia Fermata $m^n \equiv 1 \pmod{p}$. Zatem powyższe dwa równania dają $-\left(t + \frac{1}{2}\right) \equiv 1 \pmod{p}$

Zastępując t przez jego wartość i upraszczając uzyskujemy

$$\frac{2m-1}{p} + 2 \equiv 0 \pmod{p}.$$

Ponieważ $2m-1$ jest nieparzyste implikuje to, że $2m-1$ jest wolnym kwadratem. Mnożenie kongruencji powyższego typu, po jednej dla każdego r pierwszego dzielnika $2m-1$ otrzymamy

$$2^{r-1} \left((2m-1) \sum_{p|(2m-1)} \frac{1}{p} + 2 \right) \equiv 0 \pmod{2m-1}.$$

Ponieważ moduł jest nieparzysty daje to

$$\sum_{p|(2m-1)} \frac{1}{p} + \frac{2}{2m-1} \equiv 0 \pmod{1}.$$

W końcu uzyskujemy odpowiednią kongruencję dla pierwszego podzielnika $2m+1$. Dla tego celu zapiszemy postać

$$S_n(m+1) = 2m^n$$

Przypuśćmy, że $p | 2m+1$. Ustawmy $v = \frac{1}{2} \left(\frac{2m+1}{p} - 1 \right)$. Używając argumentu odkryjemy, że $(p-1) | n$ i $2m+1$ jest wolnym kwadratem. Na końcu uzyskujemy

$$\sum_{p|(2m+1)} \frac{1}{p} + \frac{4}{2m+1} \equiv 0 \pmod{p}.$$

Załóżmy ponownie, że $m+1$ jest parzyste. Jeśli teraz dodamy lewe strony

$$\sum_{p|(m-1)} \frac{1}{p} + \frac{1}{m-1} \quad \sum_{p|(m+1)} \frac{1}{p} + \frac{2}{m+1} \quad \sum_{p|(2m+1)} \frac{1}{p} + \frac{4}{2m+1} \quad \sum_{p|(2m-1)} \frac{1}{p} + \frac{2}{2m-1}$$

uzyskamy liczbę całkowitą przynajmniej 4. Żadna liczba pierwsza $p > 3$ nie może być dzielona więcej niż raz przez liczby $m-1$, $m+1$, $2m-1$, $2m+1$. Dalej 2 i 3 mogą być dzielone więcej niż dwa przez te liczby. Zatem, jeśli $M = (m-1)(m+1)(2m-1)(2m+1)$ wtedy

$$\sum_{p|M} \frac{1}{p} + \frac{1}{m-1} + \frac{2}{m+1} + \frac{2}{2m-1} + \frac{4}{2m+1} \geq 4 - \frac{1}{2} - \frac{1}{3}.$$

Widzieliśmy już, że jedyną możliwością dla m z $m \leq 1000$ są 3, 7 i 43.

Lemat 2

$$\sum_{p \leq 10^7} \frac{1}{p} < 3.16$$

Dowód Przez bezpośrednie obliczenie

$$\sum_{p \leq 10^8} \frac{1}{p} < 2.18.$$

Z tablicy Lehmera i wyraźnych szacunków dla $\pi(x)$ ze względu na Rosnera, łatwo można sprawdzić, że dla $10^3 < x < 10^7$,

$$\pi(x) < \frac{1.2x}{\log x}.$$

VII. Kombinatoryczna Teoria Liczb

Istnieje wiele interesujących pytań, które leżą pomiędzy teorią licza a analizą kombinatoryczną. Rozważmy jedno z nich, które postawił I.Schur (1917) i związane jest w zaskakujący sposób z Twierdzeniem Fermata. Ogólnie rzecz biorąc, twierdzenie Schura stanowi, że jeśli n jest stałe i wystarczająco wiele kolejnych liczb całkowitych $1, 2, 3, \dots$ podzielonych na klasy n , wtedy przynajmniej jedna klasa będzie zawierała elementy a, b, c , z $a+b=c$. Rozważmy fakt, że jeśli oddzielimy dodatnie liczby całkowite mniejsze niż 2^n na n klas przez wstawienie 1 w klasie 1, następnie 2 w klasie 2, następnie 4 w klasie 3, itd, wtedy żadna klasa nie zawiera sumy dwóch swoich elementów. Alternatywnie, możemy zapisać każdą liczbę całkowitą m w postaci $2^k \theta$ gdzie θ jest nieparzyste, i umieścić m w k -tej klasie. Ponownie liczba mniejsza niż 2^n będzie leżała w n klasach i jeśli $m_1 = 2^{k_1} \theta_1$ a $m_2 = 2^{k_2} \theta_2$ są w klasie k wtedy $m_1 + m_2 = 2^k(\theta_1 + \theta_2)$ leży w wyżej numerowanej klasie. Bardziej skomplikowany sposób dystrybucji liczb całkowitych przedstawionych poniżej pozwala na dystrybucję $1, 2, \dots, 3^n - 1/2$ na n klas w taki sposób, że żadna klasa nie ma rozwiązania $a+b=c$:

$$\begin{array}{ccc} 1 & 2 & 5 \\ 3 & 4 & 6 \\ 10 & 11 & 7 \\ 13 & 12 & 8 \\ \vdots & \vdots & \vdots \end{array}$$

Z drugiej strony, twierdzenie Schura stanowi, że jeśli jeden oddziela liczby $1, 2, 3, \dots, [n!e]$ na n klas w jakikolwiek sposób przynajmniej jedna klasa będzie zawierała rozwiązanie $a+b=c$. Różnica między ostatnimi dwoma wyrażeniami ujawnia interesujący nierozwiązany problem, mianowicie, czy można zastąpić $[n!e]$ w wyniku Schura przez rozsądną mniejszą liczbą? Pierwsze dwa przykłady wykazują, że z pewnością nie możemy zejść niżej jak $2^n - 1$, a ostatni przykład przykłady pokazuje, że nie możemy zejść niżej $3^n - 1/2$. Teraz podamy definicję i stworzymy kilka uwag aby ułatwić dowód twierdzenia Schura

Niech $T_0 = 1$, $T_n = nT_{n-1} + 1$. Łatwo sprawdzić, że

$$T_n = n! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} \right) = [n!e].$$

Tak więc twierdzenie Schura może być rozwinięte tak: Jeśli $1, 2, \dots, T_n$ są podzielone na n klas w jakikolwiek sposób, przynajmniej jedna klasa będzie zawierała rozwiązanie $a+b=c$. Udowodnimy to przez założenie, że liczby $1, 2, \dots, T_n$ skasyfikowano na n sposobów bez klasy zawierającej

rozwiązania $a+b=c$ i uzyskując z tego sprzeczność. Zwróć uwagę, że warunek $a+b \neq c$ oznacza, że żadna klasa nie może zawierać różnicy dwóch ich elementów. Przypuśćmy, że jakaś klasa, powiedzmy A zawiera elementy $a_1 < a_2 < \dots$. Tworzymy ich różnice w następujący sposób

$$\begin{aligned} b_1 &= a_2 - a_1, & b_2 &= a_3 - a_1, & b_3 &= a_4 - a_1, & \dots \\ c_1 &= b_2 - b_1, & c_2 &= b_3 - b_1, & c_3 &= b_4 - b_1, & \dots \\ d_1 &= c_2 - c_1, & d_2 &= c_3 - c_1, & d_3 &= c_4 - c_1, & \dots \end{aligned}$$

i tak dalej. Zauważmy, że wszystkie b, c, d itd różnią się od a a zatem nie mogą leżeć w A . Teraz zaczniemy z T_n elementami. Co najmniej

$$\left\lfloor \frac{T_n}{n} + 1 \right\rfloor = T_{n-1} + 1$$

z nich musi leżeć w pojedynczej klasie, powiedzmy A_1 . Wtedy formujemy T_{n-1} b. Te nie leżą w A_1 a zatem leżą w pozostałych $n-1$ klasach. Co najmniej

$$\left\lfloor \frac{T_{n-1}}{n-1} + 1 \right\rfloor = T_{n-2} + 1$$

z nich musi leżeć w pojedynczej klasie, powiedzmy A_2 . Formujemy ich T_{n-2} różnice, c . Te dają T_{n-2} liczb albo w A_1 albo A_2 . Kontynuując w ten sposób dostajemy T_{n-3} liczb nie w A_1, A_2, A_3 . W ten sposób ewentualnie uzyskujemy $T_0 = 1$ liczb nie należących do A_1, A_2, \dots, A_n . Ale wszystkie liczby tworzy się między liczbami $1, 2, \dots, T_n$ tak więc mamy sprzeczność, która udowadnia twierdzenie. Określimy, bez udowadniania, związek z twierdzeniem Fermata. Naturalnym podejściem do twierdzenia Fermata będzie próba wykazania, że $x^n + y^n = z^n \pmod{p}$ jest nierozwiązywalne modułem jakiegoś p , o ile p nie dzieli $x*y*z$. Jednak twierdzenie Schura może być użyte do wykazania, że ta metoda musi być błędna i rzeczywiście jeśli $p > n!$ wtedy $x^n + y^n = z^n \pmod{p}$ ma rozwiązanie z p nie współczynnikiem x, y, z . Nieco podobne do twierdzenia Schura jest znane twierdzenie Van der Waerdena, które pokrótce zbadamy. Na początku lat dwudziestych powstał następujący problem w związku z dystrybucją reszt kwadratowych. Wyobraź sobie, że zbiór wszystkich liczb całkowitych podzielonych w jakiś sposób na dwie klasy, Czy można twierdzić, że rozkład arytmetyczny dowolnej długości może być znaleziony przynajmniej dla jednej z tych klas? Problem pozostał nierozwiązany od lat, mimo skoncentrowanych wysiłków wielu wybitnych matematyków. Został w końcu rozwiązany przez Van der Waerdena w 1928 roku. Ponieważ nie jest niczym niezwykłym przy takich problemach, pierwszym krokiem Van der Waerdena było uczynienie tego problemu bardziej ogólnym a tym samym łatwiejszym. Van der Waerden udowodnił następująco: Dane liczby całkowite k i l , istnieje liczba całkowita $W = W(k, l)$ taka, że jeśli liczby $1, 2, 3, \dots, W$ są podzielone na k klas w dowolny sposób, wtedy przynajmniej jedna klasa będzie zawierała l warunków w rozkładzie arytmetycznym. Nie podamy tu dowodu Van der Waerdena. Jest niezwykle trudny i prowadzi tylko do fantastycznie dużych granic dla $W(k, l)$. Z tego powodu czytelnik może rozważyć wartość rozważenia nierozwiązany problem znajdowania alternatywnie prostszych dowodów, że $W(k, l)$ istnieje i znaleźć rozsądne granice dla niej. Będziemy mieli więcej do powiedzenia o funkcji $W(k, l)$ trochę później. Nasz kolejny problem z kombinatorycznej teorii liczb jest to sekwencja "nonaveraging". Wywołajmy sekwencję $A: a_1 < a_2 < a_3 < \dots$ nie średnią jeśli nie zawiera średnią z dwóch jego elementów tj $a_i + a_j \neq 2a_k$ ($i \neq j$). Niech $A(n)$ oznacza liczbę elementów w A nie przekraczającą n . Główny problem to oszacowanie jak duże może być $A(n)$ jeśli A nie jest nieśrednią. Możemy sformować nieśrednią sekwencję zaczynając od $1, 2, \dots$ a potem zawsze biorąc najmniejszą liczbę, która nie narusza warunku nieśredniego zbioru. W ten sposób uzyskujemy $1, 2, 4, 5, 10, 11, 13, 14, 28, 29, 31, \dots$. Interesującym faktem jest, że ta sekwencja jest związana z trójkowym zbiorem Cantora. Rzeczywiście, pozostawimy to jako ćwiczenie, udowodnienie, że ta sekwencja może być uzyskiwana przez dodanie 1 do każdej liczby całkowitej

która reprezentuje w podstawie 3 zawierającej tylko 0 lub 1. Sekwencja ta jest maksymalna w tym sensie, że żadna nowa liczba nie może być wstawiona do tej sekwencji bez niszczenia jej nieśredniego charakteru. Ten, jak również inne fakty, doprowadziły Szerekesa (około 1930 roku) do przypuszczenia, że ten zbiór był tak gęsty jak każdy nieśredni zbiór. Dla tego zbioru, funkcja zliczania może być łatwo oszacowana $\sim n^{\log 2 / \log 3}$. Dlatego pojawiło się znaczne zaskoczenie gdy Salem i Spencer (1942 rok) udowodnili, że można mieć nieśredni zbiór liczb całkowitych $\leq n$ zawierający przynajmniej

$$n^{1-c/\sqrt{\log \log n}}$$

możemy zdecydować czy x jest w R na podstawie następujących zasad

Po pierwsze musimy dołączyć zbiór x w zbiorze nawiasów, stawiając pierwsze cyfry (licząc od prawej do lewej) w pierwszym nawiasie, kolejne dwie w drugim nawiasie, kolejną trzy w trzecim nawiasie i tak dalej. Jeśli ostatni niepusty nawias (nawias najdalej na lewo, który nie składa się wyłącznie z zer) nie ma maksymalnej liczby cyfr, możemy wypełnić go zerami. Na przykład liczby

$$a = 32653200200, \quad b = 100026000150600, \quad c = 1000866600290500$$

można zanawiasować tak

$$a = (00003)(2653)(200)(20)(0)$$

$$b = (10002)(6100)(150)(60)(0)$$

$$c = (10008)(6600)(290)(50)(0)$$

odpowiednio. Teraz przypuśćmy, że r -ty nawias w z zawiera niezerowe cyfry, ale wszystkie dalsze nawiasy na lewo są 0. Wywołajmy liczbę przedstawiającą cyfry w i -tym nawiasie x_i , $i=1,2,\dots,r-2$. Dalej, oznaczmy przez \bar{x} liczbę przedstawianą przez cyfrę w ostatnich dwóch nawiasach wziętą razem, ale wykluczając ostatnią cyfrę. Dla x należącego do R wymagamy

- (1) ostatnia cyfra x musi być 1
- (2) x_i musi zaczynać się od 0 dla $i=1,2,\dots,r-2$
- (3) $x_1^2 + \dots + x_{r-2}^2 = \bar{x}$

W szczególności, zwróć uwagę, że a spełnia (2) ale narusza (1) i (3) tak więc a nie jest w R ; ale b i c spełniają wszystkie trzy warunki i są w R . Aby sprawdzić (3) odnotuj, że $60^2 + 150^2 = 26100$.

Następnie udowodnimy, że żadna z trzech liczb całkowitych w R nie jest w rozkładzie arytmetycznym. Po pierwsze odnotuj, że jeśli dwa elementy z R mają różne liczby niepustych nawiasów ich średnia nie może spełniać (1). Zatem, musimy tylko rozważyć średnie elementów z R mają tę samą liczbę niepustych nawiasów. Z (1) i (3) wynika, że te dwa elementy z R mogą być średnimi nawiasom przez nawiasy dla pierwszych $r-2$ nawiasów i również dla ostatnich dwóch nawiasów wziętych razem. Zatem w naszym przykładzie

$$\frac{1}{2}(60 + 50) = 55, \quad \frac{1}{2}(150 + 290) = 220,$$

$$\frac{1}{2}(100026100 + 100086600) = 100056350,$$

$$\frac{1}{2}(b + c) = (10005)(6350)(220)(55)(0)$$

To narusza (3) i nie jest w R . Genralnie udowodnimy, że jeśli x i y są w R wtedy $\bar{z} = \frac{1}{2}(x + y)$

narusza (3) i nie jest w R
Ponieważ x i y są w R

$$\bar{z} = \frac{\bar{x} + \bar{y}}{2} = \sum_{i=1}^{r-2} \frac{x_i^2 + y_i^2}{2}$$

Z drugiej strony z w R implikuje

$$\bar{z} = \sum_{i=1}^{r-2} z_i^2 = \sum_{i=1}^{r-2} \frac{(x_i + y_i)^2}{2}$$

Stąd jeśli z jest w R wtedy

$$\sum_{i=1}^{r-2} \frac{x_i^2 + y_i^2}{2} = \sum_{i=1}^{r-2} \frac{(x_i + y_i)^2}{2}$$

Zatem

$$\sum_{i=1}^{r-2} \frac{(x_i - y_i)^2}{2} = 0,$$

co implikuje $x_i = y_i$ dla $i = 1, 2, \dots, r-2$. To razem z (1) i (2) implikuje, że x i y nie są różne. Sekwencja Szerekesa zaczyna się od 1,2,4,5,10,11,..... Nasza sekwencja zaczyna się od

100000, 1000100100, 1000400200,

Niemniej jednak warunki naszej sekwencji są znacznie mmniejsze niż te odpowiadające warunkom sekwencji Szerekesa. Teraz oszacujemy ile liczb całkowitych w R zawiera dokładnie r nawiasów. Biorąc pod uwagę r nawiasów możemy sprawić, że pierwsza cyfra w każdym r-2 nawiasów to 0. Możemy wypełnić pierwsze r-2 nawiasy w sposób arbitralny. To może być zrobione na

$$10^{0+1+2+\dots+(r-2)} = 10^{\frac{1}{2}(r-1)(r-2)}$$

sposobów. Ostatnie dwa nawiasy mogą być wypełnione w taki sposób aby spełniały (1) i (3). Aby zobaczyć to musimy tylko sprawdzić, że ostatnie dwa nawiasy nie będą przepełnione, i że ostatnie dwie cyfry, które ustawiliśmy na 1, nie będą z nimi interferować. Wynika to z nierówności

$$(10^1)^2 + (10^2)^2 + \dots + (10^{r-2})^2 < 10^{2(r-1)}$$

Dla danego n niech r będzie liczbą całkowitą określoną przez

$$10^{\frac{1}{2}r(r+1)} \leq n < 10^{\frac{1}{2}(r+1)(r+2)} \quad (1)$$

Ponieważ wszystkie liczby całkowite z większością r na $10^{\frac{1}{2}(r-2)(r-1)}$ przekraczać n, a ponieważ r nawiasów może być wypełnionych do specyfikacji na $10^{\frac{1}{2}(r-1)(r-2)}$ sposobów, mamy

$$R(n) \geq 10^{\frac{1}{2}(r-1)(r-2)} \quad (2)$$

Po prawej stronie (1) mamy

$$r + 2 > \sqrt{2 \log n}$$

więc (2) implikuje ,że

$$R(n) \geq 10^{\frac{1}{2}(r-1)(r-2)} > 10^{\log n - c\sqrt{\log n}} > 10^{(\log n)(1 - c/\sqrt{\log n})}$$

gdzie wszystkie logarytmy są o podstawie 10

Stare domysły były takie ,że $\frac{A(n)}{n} \rightarrow 0$ dla każdej nieśredniej sekwencji. Zostało to udowodnione w 1954 roku przez K.F.Rotha. Jego dowód nie jest elementarny. L.Moser użył podobnej techniki dla uzyskania niższej granicy dla funkcji $W(k,l)$ Van der Waerdena. Udowodnił ,że $W(k,l) > lk^{\log k}$, tj wykazał ,jak rozłożyć liczby $1,2,\dots,[lk^{\log k}]$ na k klas w taki sposób, że żadna klasa zawierająca 3 warunki w rozkładzie arytmetycznym. Używając całkiem różnych metod Erdos i Rado wykazali ,że $W(k,l) > \sqrt{2}lk^l$. Erdos podniósł następująca kwestię: Jaka jest maksymalna liczba całkowitych $a_1 < a_2 < \dots < a_k \leq n$ taka ,że 2^k sumy różnych a wszystkie są różne? Potęgi 2 pokazują ,że jedna może dać $k+1$ a nie przekraczający 2^k a jedna może faktycznie dać $k+2$ a ponad 2^k spełniające wymagany warunek. Z drugiej strony, wszystkie sumy są mniejsze niż kn tak więc

$$2^k \leq kn, \quad (1)$$

co implikuje

$$k < \frac{\log n}{\log 2} + (1 + o(1)) \frac{\log \log n}{\log 2}. \quad (2)$$

Teraz pokażemy jak Erdos i Moser poprawili te szacunki do

$$2^k < 4\sqrt{kn}, \quad (3)$$

co implikuje

$$k < \frac{\log n}{\log 2} + (1 + o(1)) \frac{\log \log n}{2 \log 2}. \quad (4)$$

Przy założeniu Erdosa jest takie

$$k = \frac{\log n}{\log 2} + o(1). \quad (5)$$

Oznaczmy sumę różnych a przez s_1, s_2, \dots, s_{2^k} i niech $A = a_1 + a_2 + \dots + a_k$. Zauważ że średnia suma to $A/2$ ponieważ możemy zsumować każdą parę z sumą komplementarnego zbioru .Sugeruje to ,że szacunek $\frac{1}{2^k} \sum_i (s_i - \frac{A}{2})^2$.

Mamy

$$\sum_i \left(s_i - \frac{A}{2} \right)^2 = \sum \frac{1}{2} (\pm a_1 \pm a_2 \pm \dots \pm a_k)^2$$

gdzie ostatnia suma przebiega przez 2^k możliwych rozkładów znaku. Przy podnoszeniu do kwadratu odkryjemy, że wszystkie krzyżowe warunki przychodzą w parach gdzie każdy a_i^2 pojawi się 2^k razy
Zatem

$$\sum_i \left(s_i - \frac{A}{2} \right)^2 = 2^k \sum a_i^2 < 2^{k-2} n^2 k$$

Zatem liczba sum s_i dla których

$$\left| s_i - \frac{A}{2} \right| \geq n\sqrt{k}$$

nie może przekraczać 2^{k-1} . Ponieważ wszystkie sumy są inne, mamy 2^{k-1} różnych liczb w zakresie długości $2n\sqrt{k}$. Daje to $2^{k-1} \leq 2n\sqrt{k}$ jak wymagano. Niech $a_1 < a_2 < \dots$ będzie nieskończoną sekwencją liczb całkowitych a zdefiniowane $f(n)$ będzie liczbą rozwiązań z $n = a_i + a_j$ gdzie wszystkie rozwiązania liczy się raz. G.A. Dirac i D.J. Newman podali interesujący dowód, że $f(n)$ nie może być stała na jakimś etapie. Jeśli $f(1+1) = f(1+1) = \dots$ będziemy mieli

$$\begin{aligned} \frac{1}{2} \left(\sum z^{a_k} \right)^2 + \sum z^{2a_k} &= \sum f(n) z^n \\ &= P_\ell(z) + a \frac{z^{\ell+1}}{1-z}, \quad (f(\ell+1) = a) \end{aligned}$$

gdzie $P(z)$ jest wielomianem stopnia $\leq \ell$. Jeśli $z \rightarrow -1$ na osi rzeczywistej po prawej stronie pozostaje ograniczony, ale z lewej strony dąży do nieskończoności, ponieważ oba warunki po lewej stronie są dodatnie a drugi zmierza do nieskończoności. Ta sprzeczność dowodzi twierdzenia. Turan i Erdos przypuszczali, że jeśli $f(n) > 0$ dla wszystkich wystarczająco dużych n wtedy $\limsup f(n) = \infty$ ale to wydaje się bardzo trudne do udowodnienia. Jeszcze silniejsze domysły były, że jeśli $a_k > ck^2$ wtedy $\limsup f(n) = \infty$. Najlepszym znanym wynikiem w tym kierunku jest tylko $\limsup f(n) \geq 2$.

Fuchs i Erdos udowodnili, że

$$\sum_{k=1}^n f(k) = cn + o\left(\frac{n^{\frac{1}{4}}}{\log n}\right)$$

jest niemożliwe. Jeśli $a_k = k^2$ przychodzi do problemu punktów siatki w okręgu o promieniu n . Hardy i Landau udowodnili, że

$$\sum_{k=1}^n f(k) = \pi n + o(n \log n)$$

nie posiada. Choć nie tak silny jak ten, wynik Erdosa i Fuchsa ma zastosowanie do dużo bardziej ogólnych sytuacji i jest dużo łatwiejszy (ale nie bardzo łatwy) do udowodnienia.

Niech $a_1 < a_2 < \dots$ będzie nieskończoną sekwencją liczb całkowitych. Erdos przypuszczał a G.G. Lorentz udowodnił, że istnieje sekwencja $\{b_i\}$ zerowej gęstości taka, że każda liczba całkowita jest

w postaci $a_i + b_j$. Interesującym nierozwiązanym problemem w tym kierunku jest znalezienie sekwencji $B: b_1 < b_2 < \dots$ z funkcją zliczającą $B(n) < cn / \log n$ taką, że każda liczba całkowita jest w postaci $2^k + b_j$. Niech $a_1 < a_2 < \dots < a_{2n}$ będzie $2n$ liczbami całkowitymi w przedziale $[1, 4n]$ a $b_1 < b_2 < \dots < b_{2n}$ pozostałymi liczbami w tym przedziale. Erdos przypuszczał, że istnieje liczba całkowita x taka, że liczba rozwiązań $a_i + x = b_j$ jest to co najmniej n . Całkiem łatwo wykazać, że istnieje x takie, że liczba rozwiązań $a_i + x = b_j$ to przynajmniej $n/2$. Obserwujemy, że liczba rozwiązań $a_i + y = b_j$ to $4n^2$ i, że jest $8n$ możliwych wyborów z y tj $-4n \leq y \leq 4n$, $y \neq 0$. Zatem dla pewnego y_0 jest przynajmniej $n/2$ b w $a_i + y_0$. P.Scherk poprawił $n/2$ na $n(2-\sqrt{2}) = .586n$. Zupełnie inną metodą L.Moser poprawił to na $.712n$. Z drugiej strony Selfidge, Ralston i Motzkin użyli S.W.A.C dla obalenia oryginalnego przypuszczenia i znaleźli przykłady gdzie, żadna liczba nie jest reprezentowalna więcej niż $.8n$ razy jako różnica między a a b . Jeszcze inny zbiór ciekawych problemów z dziedziny kombinatorycznej teorii liczb obracają się wokół pojęcia łańcucha dodawania wprowadzony przez A.Scholza. Łańcuch dodawania dla n jest zbiorem $l = a_0 < a_1 \dots < a_r = n$ takie, że każdy element a_r może być zapisany jako suma $a_s + a_t$ poprzedzających elementów łańcucha. Na przykład dla $n = 666$

1, 2, 4, 8, 16, 24, 40, 80, 160, 320, 640, 664, 666

fromujemy łańcuch z $r = 12$; to samo dotyczy

1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 324, 648, 666.

W każdym przypadku musimy mieć $a_1=2$ i $a_2 = 3$ lub 4 . Przez długość $l = l(n)$ Scholtz rozumiał najmniejsze l dla którego istnieje łańcuch dodawania $a_0, a_1, \dots, a_l = n$ Scholtz przedstawił co następuje

$$m + 1 \leq \ell(n) \leq 2m \text{ for } 2^m + 1 \leq n \leq 2^{m+1} \quad (m \geq 1)$$

$$\ell(ab) \leq \ell(a) + \ell(b);$$

$$\ell(2^{m+1} - 1) \leq m + \ell(m + 1).$$

Pierwsze dwa są łatwe do udowodnienia. Trzeci przypuszczalnie będzie fałszywy. Scholtz przypuszczał, że pierwsze może być poprawione i podwyższone do pytania czy lub nie

$$1 \leq \limsup_{n \rightarrow \infty} \frac{\ell(n)}{\log_2 n} \leq 2$$

może być poprawione.

W dalszej części udowodnimy i damy zarys dowodu A,Brauera, że

$$\ell(n) \sim \log_2 n.$$

Założmy, że liczby całkowite są zapisane o podstawie 2 i szukamy łańcucha dodawania powiedzmy dla 10110110. Możemy sformować łańcuch

1, 10, 100, 101, 1010, 1011, 10110, 101100, 101101, 1011010,
1011011, 10110110, 101101100, 101101101.

W tym procesie, każda cyfra "kosztuje" przynajmniej dwa elementy w łańcuchu, tak więc $l < 2\log_2 n$. Ponieważ lewa strona nierówności (1) jest trywialną metodą wskazania powyżej danego dowodu (1). Ideą Brauera jest zbudowanie dużego stosu liczb najpierw a użycie go kiedy nadarzy się okazja. Założmy n o 2^m . Zacniemy z łańcuchem $1, 2, \dots, 2^r$, gdzie r będzie określone później. Teraz podzielić cyfry n na m/r bloków z r cyframi w każdym bloku. Na przykład założmy

$$n = (101)(110)(010)(101)(111)$$

Tu $m = 15$, $r = 3$

Zaczynając od naszego stosu wszystkich 3 cyfrowych liczb możemy postępować w następujący sposób

1, 10, 100, 101, 1010, 10100, 101000, 101110,
1011100, 10111000, 101110000, 101110010, ...

gdzie między etapami podkreślenia podwajamy i na podkreślonych etapach dodajemy właściwe liczby z naszego stosu dla zbudowania n . W tym przypadku potrzebujemy $2^3 + 2^{15} + 5$ kroków. Ogólnie, liczba kroków dla liczb powyżej 2^m powinna być około $2^r + m + m/r$. Przez właściwy wybór r możemy stworzyć $2^r + m/r$ tak małe jak potrzebujemy w porównaniu z m . Rzeczywiście, używając tego pomysłu Brauera udowodnił ogólnie

$$\ell(n) < \log_2 n \left\{ 1 + \frac{1}{\log \log n} + \frac{2 \log 2}{(\log n)^{1-\log 2}} \right\}$$