Kongruencje – twierdzenie Wilsona

Kongruencje – Wykład 5

Twierdzenie Wilsona. . .

pojawia się po raz pierwszy – bez dowodu – w *Meditationes Algebraicae* Edwarda Waringa (1770), profesora (*Lucasian Professor*) matematyki w Cambridge, znanego głównie z *hipotezy Waringa*, o której jeszcze powiemy.
Wilson, który zresztą poświęcił się później prawu, był jednym z uczniów Waringa. Pierwszy dowód twierdzenia przeprowadził Lagrange (też 1770). Nie używając języka kongruencji –

wyrażenie $(p-1)!+1$ jest podzielne przez p,

albo – w języku kongruencji

Wilson

Dla każdej liczby pierwszej p

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

na przykład. . .

$4! \equiv -1 \pmod 5$, $6! \equiv -1 \pmod 7$, $10! \equiv -1 \pmod{11}$, $18! \equiv -1 \pmod{19}$, itd

Twierdzenie Wilsona – dowód

Dla udowodnienia wystarczy zauważyć, że jeżeli resztę z dzielenia przez p oznaczymy przez a: $a = 1, 2, \ldots, p-1$ to kongruencja liniowa

$$ax \equiv 1 \pmod{p}$$

ma dokładnie jedno rozwiązanie ($d = (a, p) = 1$) modulo p,
liczbę b taką że $ab \equiv 1 \pmod{p}$.
Liczby a i b muszą „parami” wystąpić w zbiorze reszt modulo p.
Zauważmy, że przypadek $a = b$ może być zrealizowany tylko jeżeli

$x^2 \equiv 1 \pmod{p}$, $\rightarrow$ $(x-1)(x+1) \equiv 0 \pmod{p}$ $\rightarrow$ $x \equiv \pm 1 \pmod{p}$.

Wymnażając wszystkie reszty $a = 1, 2, \ldots, p-1$ dostajemy z jednej strony $(p-1)!$, a z drugiej – iloczyn $(p-1)/2 - 1$ par, których iloczyny przystają do 1 modulo p i jedną parę 1 i $p-1$, której iloczyn przystaje modulo p do -1. $\square$.

Dla modułów złożonych mamy wariant . . .

. . . twierdzenie

$$(m-1)! \equiv 0 \pmod{m}; \quad m > 4.$$

Rzeczywiście, jeżeli $m = pq$ i $p \neq q$ mamy q, $p < m$ i obie liczby muszą wystąpić w iloczynie $(m-1)!$, który w takim razie musi być podzielny przez m. Dla $m = p^2$ w iloczynie $(m-1)!$ pojawi się (dla $m > 2$) para p i $2p$. $\square$.

Twierdzenie Wilsona – ciąg dalszy

Rozpisując silnię w nieco wyszukany sposób...

$$(p-1)! = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \frac{p+1}{2} \ldots (p-2)(p-1)$$

i zauważając, że mamy kongruencje

$$p-1 \equiv -1,\ p-2 \equiv -2,\ \ldots,\ \frac{p+1}{2} \equiv \frac{p-1}{2} \pmod{p}$$

możemy zapisać

$$(p-1)! \equiv (-1)^{(p-1)/2} \left[1 \cdot 2 \cdot 3 \cdot \ldots \cdot \tfrac{p-1}{2}\right]^2 \pmod{p}.$$

Wstawiamy tak określone $p-1)!$ do twierdzenia Wilsona:

nowa postać tw. Wilsona to

$$\left[1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right]^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Twierdzenie Wilsona – ciąg dalszy

dla $p = 4n + 1 \ldots$

ostatnia równość z uwagi na $(-1)^{(p+1)/2} = \ldots - 1$ przybiera postać

$$\left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)^2 + 1 \equiv 0 \pmod{p},$$

co oznacza, że kwadratowa kongruencja $x^2 + 1 \equiv 0 \pmod{p}$ jest rozwiązywalna, a jej pierwiastki to

$$\pm\left(\frac{p-1}{2}\right)! \pmod{p}$$

Na przykład dla $p = 13$ mamy $[(p-1)/2]! = 6! \equiv 5 \pmod{13}$, a stąd $5^2 + 1 \equiv 0 \pmod{13}$.

Twierdzenie Wilsona – ciąg dalszy

dla $p = 4n + 3 \ldots$

ostatnia równość z uwagi na $(-1)^{(p+1)/2} = \ldots 1$ przybiera postać

$$\left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)^2 - 1 \equiv 0 \pmod{p},$$

albo

$$\left[\left(\frac{p-1}{2}\right)! + 1\right]\left[\left(\frac{p-1}{2}\right)! - 1\right] \equiv 0 \pmod{p},$$

co z kolei oznacza, że dla $p = 4n + 3$ musi zachodzić jedna z kongruencji

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

Dla kilku liczb pierwszych mamy:
$1! \equiv 1 \pmod{3}$, $3! \equiv -1 \pmod{7}$, $5! \equiv -1 \pmod{11}$,
$9! \equiv 1 \pmod{19}$, $11! \equiv 1 \pmod{23}$.

Kongruencje kwadratowe – przypadek specjalny

Określimy liczbę rozwiązań dla kongruencji $x^2 \equiv 1 \pmod{m}$.
Jak już pokazaliśmy, możemy to zrobić rozwiązując naszą kongruencję dla modułu będącego pewną potęgą liczby pierwszej, wchodzącą w skład rozkładu kanonicznego modułu m – a po znalezieniu wszystkich rozwiązań cząstkowych skorzystać z chińskiego twierdzenia o resztach.

Zaczynamy od kongruencji

$$x^2 \equiv 1 \pmod{p^\alpha}; \quad p > 2$$

równoważnej

$$(x-1)(x+1) \equiv 0 \pmod{p^\alpha}.$$

Dla $p > 2$ mamy oczywiste pierwiastki $x = \pm 1 \pmod{p^\alpha}$.
Dla $p = 2$, $\alpha = 1$ kongruencja $x^2 \equiv 1 \pmod{2}$ ma jeden pierwiastek modulo 2: $x = 1$.
Dla $p = 2$, $\alpha = 2$ kongruencja $x^2 \equiv 1 \pmod{4}$ ma dwa pierwiastki modulo 4: $x = \pm 1$.

Dla $p = 2$, $\alpha > 2$ ...

...w kongruencji $(x-1)(x+1) \equiv 0 \pmod{2^\alpha}$ oba czynniki są bądź nieparzyste, bądź parzyste; ale w tym drugim przypadku tylko jeden z czynników jest podzielny przez 4 (albo wyższą potęgę dwójki). Jeżeli $2 \mid (x+1)$ ale $4 \nmid (x+1)$ to drugi czynnik musi być podzielny przez $2^{(\alpha-1)}$, tak więc musi zachodzić $x \equiv 1 \pmod{2^{(\alpha-1)}}$, czyli $x = 1 + h2^{(\alpha-1)}$ a to jest równoważne dwóm różnym rozwiązaniom pierwotnej kongruencji:

$x \equiv 1, \quad x \equiv 1 + 2^{(\alpha-1)} \pmod{2^\alpha}$.

Analogicznie, jeżeli $2 \mid (x-1)$ to musi zachodzić $x \equiv -1 \pmod{2^{(\alpha-1)}}$, czyli $x = -1 + h2^{(\alpha-1)}$ – a to jest równoważne dwóm różnym rozwiązaniom pierwotnej kongruencji:

$x \equiv -1, \quad x \equiv -1 + 2^{(\alpha-1)} \pmod{2^\alpha}$.

Tak więc dla potęgi dwójki większej od 2 mamy cztery rozwiązania; dla potęgi równej dwa – dwa, i dla $\alpha = 1$ – jedno.

Kongruencje kwadratowe – przypadek specjalny, c.d.

Określamy liczbę rozwiązań dla kongruencji $x^2 \equiv 1 \pmod{m}$.
Jeżeli rozkład kanoniczny modułu ma postać

$$m = 2^{\alpha} {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$$

to dla $2 \nmid m$ mamy po dwa pierwiastki dla każdej kongruencji modulo ${p_i}^{\alpha_i}$ – co daje 2^r rozwiązań kongruencji kwadratowej.
Dla $\alpha = 1$ liczba tych rozwiązań nie zmienia się (kongruencja modulo 2 ma jedno rozwiązanie); dla $\alpha = 2$ dochodzą *dwa* pierwiastki kongruencji modulo 4 – a więc liczba rozwiązań kwadratowej kongruencji to 2^{r+1}; w końcu dla $\alpha > 2$ dochodzą *cztery* pierwiastki kongruencji modulo 2^{α} – liczba rozwiązań kwadratowej kongruencji wzrasta do 2^{r+2}. Możemy to ująć w formie ...

... tabeli:

α	liczba rozwiązań
0 lub 1	2^r
2	2^{r+1}
> 2	2^{r+2}

Gaussa uogólnienie twierdzenia Wilsona

Twierdzenie . . .

Jeżeli utworzyć iloczyn $\prod$ *wszystkich reszt, które są względnie pierwsze względem danego modułu* m*, to zachodzi*

$$\prod \equiv \pm 1 \pmod{m}.$$

Znak -1 pojawia się w trzech przypadkach:
(1)dla $m = 4$;
(2) dla $m = p^\beta$, $p > 2$; (3) dla $m = 2p^\beta$, $p > 2$.
W pozostałych przypadkach mamy znak $+$.
(N. B. dla $m = 2$ oba znaki są sobie równoważne $-+1 \equiv -1 \pmod{2}$.)

Oczywiście twierdzenie Wilsona jest szczególnym przypadkiem twierdzenia Gaussa – dla $m = p$.
Dowód – pozostawiamy Czytelnikowi. Można go przeprowadzić w sposób praktycznie identyczny jak w przypadku tw. Wilsona, określając liczbę pierwiastków kongruencji $x^2 \equiv 1 \pmod{m}$ (patrz poprzedni punkt).

Przedstawianie liczby jako sumy dwóch kwadratów

Była już o tym mowa przy zagadnieniu faktoryzacji. Wracamy jeszcze raz do przedstawiania liczby jako sumy dwóch kwadratów.

Axel Thue (1863-1922, Norweg); twierdzenie:

Niech p będzie liczba pierwszą, a k najmniejszą liczbą całkowitą większą od $\sqrt{p}$, a więc $k = \lfloor \sqrt{p} \rfloor + 1$.
Dla każdego a, $p \nmid a$ można znaleźć w zbiorze $\{1, 2, \ldots, k-1\}$ liczby x i y, takie że

$$xa \equiv \pm y \pmod{p}.$$

Na przykład: $p = 23$, $k = 5$.
Dla $a = 9$ i $a = 10$ mamy odpowiednio
$3a \equiv 4$, $\qquad 2a \equiv -3 \pmod{23}$.

Dowód twierdzenia Thue'go

Dla danego a, $p \nmid a$ tworzymy wszystkie kombinacje
$ax - y, \quad x, y \in [0, (k-1)]$.
Takich kombinacji (liczb) jest k^2. Ponieważ $k^2 > p$ to przynajmniej dwie takie liczby muszą być kongruentne modulo p.

Na przykład, niech będą to liczby $ax_1 - y_1$ i $ax_2 - y_2$. Mamy więc
(1)
$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}, \quad a(x_1 - x_2) \equiv (y_1 - y_2) \pmod{p}$$

Wartości bezwzględne różnic $(x_1 - x_2)$ i $(y_1 - y_2)$ także są zawarte w $[0, (k-1)]$, ale za wyjątkiem wartości zerowej
– gdyż dla np. $y_2 - y_1 = 0$ mielibyśmy $a(x_1 - x_2) \equiv 0 \pmod{p}$, czyli $x_1 = x_2$ – a z założenia były to liczby różne.
Kongruencja (1) to właśnie kongruencja, o której mówi teza twierdzenia Thue'go – z ewentualną „korektą" znaku. $\square$.

Przedstawianie liczby jako sumy dwóch kwadratów

Twierdzenie:

Liczba pierwsza p może być przedstawiona jako suma kwadratów, jeżeli kongruencja

$$a^2 + 1 \equiv 0 \pmod{p} \tag{2}$$

ma rozwiązanie.

Dowód: w oparciu o rozwiązanie kongruencji, liczbę a, określamy x i y o których mówi tw. Thue'go. Mnożymy (2) przez x^2:

$$x^2a^2 + x^2 \equiv y^2 + x^2 \equiv 0 \pmod{p},$$

a więc $y^2 + x^2 = tp,\ t > 0$. Ponieważ jednak

$$x^2 \leqslant (k-1)^2 < p, \quad \text{oraz} \quad y^2 \leqslant (k-1)^2 < p$$

to zachodzi $tp < 2p$, a więc $t < 2$. Jeżeli tak, to jedyna dopuszczalna wartość to $t = 1$ i

$$\boxed{p = y^2 + x^2.} \qquad \square$$

Przedstawianie liczby jako sumy dwóch kwadratów

Twierdzenie Thue'go połączone z faktem, że kongruencja (2) ma rozwiązanie zawsze dla $p = 4n + 1$ pozwala stwierdzić, że

$p = 4n + 1$ = suma dwóch kwadratów

Każda liczba pierwsza w postaci $p = 4n + 1$
może być przedstawiona jako suma dwóch kwadratów.

Jednocześnie, widzimy, że takie przedstawienie będzie niemożliwe dla $p = 4n + 3$. Można to ująć w formie

twierdzenia...

Dla liczby $N > 0$ w postaci $N = N_0 n^2$, gdzie n jest największym czynnikiem kwadratowym, warunkiem koniecznym i wystarczającym przedstawienia N jako sumy dwóch kwadratów jest brak czynników pierwszych o postaci $p = 4n + 3$ w rozkładzie liczby N_0.

Dowód – dla Czytelnika.