Twierdzenie Eulera

Kongruencje – wykład 6

Twierdzenie Eulera. . .

Euler, 1760, Sankt Petersburg

Dla każdego $a \perp m$ zachodzi kongruencja

$$\boxed{a^{\phi(m)} \equiv 1 \pmod{m}.}$$

Przypomnijmy: $\phi(m)$ to liczba reszt modulo m względnie pierwszych z m; $\phi(m) = m(1 - 1/p_1) \dots (1 - 1/p_r)$.

Przykłady

$m = 60 = 2^2 \cdot 3 \cdot 5$, $a = 23$. Mamy $\phi(60) = 60(1/2)(2/3)(4/5) = 16$.
Kongruencje modulo $m = 60$:
$23^2 = 529 \equiv -11, \quad \to \quad 23^4 \equiv 121 \equiv 1 \quad \to \quad 23^{16} \equiv 1.$

$m = 11$ — $m = p$; $\quad \phi(m) = p - 1 = 10$.
Kongruencje modulo $p = 11$: $\quad 2^{10} = (2^5)^2 \equiv (-1)^2 = 1.$ $\quad \square$

Twierdzenie Eulera — dowód

Oznaczmy $\phi(m)$ reszt względnie pierwszych z m
$r_1, r_2, \ldots, r_{\phi(m)}$. Każdą z nich mnożymy przez nasze $a \perp m$,
a następnie dzielimy tak otrzymaną liczbę przez m.
Otrzymujemy nowy układ reszt r'_i:

$$r_i a = q_i m + r'_i, \qquad i = 1, 2, \ldots, \phi(m),$$

albo jako kongruencje

$$(1) \qquad r_i a \equiv r'_i \pmod{m} \qquad i = 1, 2, \ldots, \phi(m).$$

- r'_i są względnie pierwsze z m (inaczej ich wspólny czynnik dzieliłby $r_i a$ – a te liczby są względnie pierwsze!).
- Danej „nowej” reszty r'_i nie da się otrzymać z *różnych* r_i i r_j (inaczej $r_i a \equiv r_j a \pmod{m} \quad \rightarrow \quad r_i \equiv r_j \pmod{m} \quad \rightarrow \quad r_i = r_j$).

Wymnażamy przez siebie wszystkie $\phi(m)$ kongruencji (1):

$$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r'_1 r'_2 \ldots r'_{\phi(m)} \pmod{m};$$

ponieważ jedne i drugie reszty są $\perp m$ możemy podzielić obie strony przez ich identyczny iloczyn. □

Twierdzenie Eulera – jeszcze jedna ilustracja

Weźmy: $m = 20$, $a = 7$.
$\phi(20) = \phi(2^2 \cdot 5) = 20(1 - 1/2)(1 - 1/5) = 8$.
Zbiór $\{r_i\}$, $i = 1, \ldots, 8$ to liczby: 1, 3, 7, 9, 11, 13, 17, 19.
Kongruencje modulo 20:

$$\begin{array}{cccc} 1a \equiv 7, & 3a \equiv 1, & 7a \equiv 9, & 9a \equiv 3, \\ 11a \equiv 17, & 13a \equiv 11, & 17a \equiv 19, & 19a \equiv 13 \end{array}$$

Po wymnożeniu stronami, mamy modulo 20

$$a^8 1 \cdot 3 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot \equiv 7 \cdot 1 \cdot 9 \cdot 3 \cdot 17 \cdot 11 \cdot 19 \cdot 13.$$

Twierdzenie Eulera – ważne (?) zastosowanie

Twierdzenie

Dla każdego $a \perp m$ kongruencja

$$ax \equiv b \pmod{m},$$

ma rozwiązanie w postaci

$$x \equiv ba^{\phi(m)-1} \pmod{m}.$$

Dowód – oczywisty.

przykład

$11x \equiv 9 \pmod{29}$. Mamy $\phi(29) = 28 \quad \rightarrow \quad x \equiv 9 \cdot 11^{27} \pmod{29}$.
Modulo 29: $11^2 \equiv 5; 11^4 \equiv 25 \equiv -4; 11^8 \equiv 16; 11^{16} \equiv 256 \equiv -5$.
Stąd $11^{27} \equiv 11^{16} \cdot 11^8 \cdot 11^2 \cdot 11^1 \equiv 8 \pmod{29}$
i ostatecznie $x \equiv 9 \cdot 8 \equiv 14 \pmod{29}$.

Twierdzenie Fermata

Dobre 120 lat . . .

przed (eleganckim) dowodem Eulera, Fermat, w jednym z listów do Frénicle de Bessy zauważa (z właściwą sobie bystrością, dowcipem i uwagą . . . *przysłałbym dowód, ale obawiam się, że jest trochę przydługi*. . .), że dla każdego $a \perp p$ istnieje (wcześniej czy później) taki najmniejszy wykładnik potęgowy d, dla którego $a^d - 1$ jest liczbą podzielną przez p; co więcej $d \mid p-1$
–a więc twierdzenie to zachodzi także dla $d = \phi(p)$.

Dowód tego twierdzenia podał w prawie 100 lat później Euler (1736).
W języku kongruencji

$$a^{p-1} \equiv 1 \pmod{p}, \tag{2}$$

albo dla modułu $m = p^\alpha$ $\left(\text{wówczas} \quad \phi(p^\alpha) = p^\alpha - p^{\alpha-1}\right)$:

$$a^{p^\alpha - p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}.$$

Sprawdź – na przykład czy $a^{100} \equiv 1 \pmod{101}$?

Twierdzenie Fermata – konsekwencje

Zgodnie z twierdzeniem Fermata, kongruencja $x^{p-1} \equiv 1 \pmod{p}$ ma $p-1$ różnych rozwiązań – liczb względnie pierwszych z p, a więc $x = 1, 2, \ldots, p-1$.
Stosując poznane wcześniej twierdzenie o postaci takiej liniowej kongruencji z r różnymi pierwiastkami możemy zapisać kongruencję (2) w postaci

$$(3) \quad \boxed{x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-[p-1]) \pmod{p}}.$$

Na przykład: dla $p = 5$ zachodzi

$$\begin{aligned}(x-1)(x-2)(x-3)(x-4) &\equiv (x-1)(x-2)(x+2)(x+1)\\ = (x^2-1)(x^2-4) &\equiv x^4 - 1 \pmod{5}.\end{aligned}$$

Twierdzenie Fermata – konsekwencje, c.d.

Mieliśmy ...

Kryterium Eulera

Dla $p > 2$ liczba $a \perp p$ jest resztą kwadratową modulo p wtedy i tylko wtedy gdy

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Z twierdzenia Fermata wynika

$$a^{p-1} - 1 \equiv 0 \equiv \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \pmod{p}.$$

a więc $a^{(p-1)/2} \equiv 1 \pmod{p}$ lub $a^{(p-1)/2} \equiv -1 \pmod{p}$. Jeżeli jednak a *jest resztą kwadratową* to istnieje pewne x_0, takie że $x_0^2 \equiv a \pmod{p}$ i wówczas

$$a^{(p-1)/2} \equiv \left(x_0^2\right)^{(p-1)/2} \equiv (x_0)^{(p-1)} \equiv 1 \pmod{p}. \qquad \square$$

Twierdzenie Fermata, a kryterium Eulera, c.d.

Implikacja odwrotna: przypuśćmy, że

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Zgodnie z twierdzeniem Lagrange'a wielomian $f(x) = x^{(p-1)/2} - 1$ nie może mieć więcej niż $(p-1)/2$ pierwiastków, różnych modulo p.

Pierwiastkami tego wielomianu – a więc możliwymi wartościami $a = x_0^2$ – mogą być tylko liczby: 1^2, 2^2, $\ldots$ $[(p-1)/2]^2$,

— są to wszystko reszty kwadratowe modulo p

i *wyczerpują wszystkie możliwości modulo* p dla liczby x_0, którymi są liczby: $\pm 1^2$, $\pm 2^2$, $\ldots$ $\pm\,[(p-1)/2]^2$. □

Twierdzenie Fermata – konsekwencje, c.d.

mieliśmy twierdzenie ... dla $b \perp m$; $a, c > 0$; jeżeli

$b^a \equiv 1 \pmod{m}$ i $b^c \equiv 1 \pmod{m} \rightarrow b^d \equiv 1 \pmod{m}$,
$d = (a, c)$.

dowód: $d = ax + cy$ – podstawiamy:
$b^d = b^{ax+cy} = = (b^a)^x \cdot (b^c)^y \equiv 1 \pmod{m}$. □

...z którego wynikało kolejne twierdzenie
Jeżeli liczba pierwsza p dzieli $N = b^n - 1$ to
(1) albo $p \mid b^d - 1$, gdzie $d \mid n$; albo
(2) $p \equiv 1 \pmod{n}$. Dla $p > 2$ i dla $n = 2k + 1$ mamy $p \equiv 1 \pmod{2n}$.

dowód: $b^n \equiv 1 \pmod{p}$ oraz $b^{p-1} \equiv 1 \pmod{p}$.
Z poprzedniego twierdzenia wynika, że $b^d \equiv 1 \pmod{p}$,
gdzie $d = (n, p - 1)$.
Jeżeli $d < n$ to $p \mid b^d - 1$ [przypadek (1)].
Jeżeli $d = n$ to $d \mid p - 1$, a więc $p \equiv 1 \pmod{n}$.
Jeżeli obie liczby p i n są nieparzyste i $n \mid p - 1$ to $2n \mid p - 1$ [przypadek (2)]. Na przykład jeżeli liczba $2^{11} - 1$ ma mieć dzielnik p to – na mocy ostatniego twierdzenia – $p = k \cdot 22 + 1$ – rzeczywiście $2047 = 23 \cdot 89$. $(p < \sqrt{(N)!})$.

Mieliśmy – równanie (3)

$$\boxed{x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-[p-1]) \pmod{p}}.$$

Wymnażając wszystkie $p-1$ czynników po prawej stronie otrzymujemy różne potęgi x-a – z różnymi współczynnikami, które przystają (modulo p) do pojawiających się po lewej stronie: jedynki (współczynnik przy x^{p-1}); -1 (wyraz wolny) i zera (pozostałe $p-2$ przypadki).
W szczególności występujący po prawej stronie wyraz wolny to

$$(-1)(-2)\dots(x-[p-1]) = (-1)^{p-1}(p-1)!,$$

a więc mamy

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

Twierdzenie Wilsona może być więc traktowane jako wniosek z twierdzenia Fermata (szczególnego przypadku tw. Eulera) – w naszym jednak wykładzie zachowaliśmy bardziej „historyczną” sekwencję.

Twierdzenie Fermata – wersja szersza

Jeżeli wyjściową kongruencję (2), zachodzącą dla $a \perp m$

$$a^{p-1} \equiv 1 \pmod{p},$$

pomnożyć przez a to dostajemy

$$a^p \equiv a \pmod{p}, \tag{4}$$

która jest słuszna *dla wszystkich liczb* a – nie tylko tych, które są względnie pierwsze z modułem p.

małe twierdzenie

W systemie dziesiętnym każda liczba ma taką samą ostatnią cyfrę jak jej piąta potęga.

Czyli:

$$a^5 \equiv a \mod 10.$$

Prościutki dowód zostawiamy Czytelnikowi (wskazówka: $a^5 \equiv a \pmod 2$).

Rząd liczby całkowitej

Z twierdzenia Fermata (Eulera) wynika, że dla każdej liczby a, która jest względnie pierwsza z modułem m *musi* istnieć wykładnik potęgowy n, dla którego $a^n \equiv 1 \pmod{m}$.

Definicja

Rzędem liczby a modulo m nazywamy *najmniejszą liczbę* naturalną r taką, że $a^r \equiv 1 \pmod{m}$. Oznaczamy ją $\mathrm{ord}_m(a)$, lub $\mathrm{ord}(a, m)$.
Uwaga: jeszcze stosunkowo niedawno dla określenia $\mathrm{ord}_m(a)$ używano *wyłącznie* terminu *wykładnik potęgowy, do którego liczba a należy modulo m.*

Przykład

dla $m = 30$ i $a = 7$. Obliczamy kolejne potęgi a modulo m
$a \equiv 7; \quad a^2 \equiv -11; \quad a^3 \equiv 13; \quad a^4 \equiv 1.$
Tak więc 4 jest rzędem liczby $a = 7$ modulo $m = 30$.

Tabela: Szukanie rzędu liczby a modulo 13.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	**3**	6	12	11	9	5	10	7	**1**
3	9	**1**	3	9	1	3	9	1	3	9	1
4	3	12	9	10	**1**	4	3	12	9	10	1
5	12	8	**1**	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	**1**
7	10	5	9	11	12	6	3	8	4	2	**1**
8	12	5	**1**	8	12	5	1	8	12	5	1
9	3	**1**	9	3	1	9	3	1	9	3	1
10	9	12	3	4	**1**	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	**1**
12	**1**	12	1	12	1	12	1	12	1	12	1

Z tabeli na poprzedniej stronie wynika:

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	**1**
3	9	**1**	3	9	1	3	9	1	3	9	1
4	3	12	9	10	**1**	4	3	12	9	10	1
5	12	8	**1**	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	**1**
7	10	5	9	11	12	6	3	8	4	2	**1**
8	12	5	**1**	8	12	5	1	8	12	5	1
9	3	**1**	9	3	1	9	3	1	9	3	1
10	9	12	3	4	**1**	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	**1**
12	**1**	12	1	12	1	12	1	12	1	12	1

$\mathrm{ord}_{13}(1) = 1;$
(tak będzie dla każdego a i m!)
$\mathrm{ord}_{13}(2) = \mathrm{ord}_{13}(6) = \mathrm{ord}_{13}(7)$
$= \mathrm{ord}_{13}(11) = 12$
$\mathrm{ord}_{13}(3) = \mathrm{ord}_{13}(9) = 3$
$\mathrm{ord}_{13}(4) = \mathrm{ord}_{13}(10) = 6$
$\mathrm{ord}_{13}(5) = \mathrm{ord}_{13}(8) = 4$
$\mathrm{ord}_{13}(12) = 2$

1. wszystkie te liczby:
   1, 2, 3, 4, 6 i 12
   to dzielniki d liczby
   $12 = 13 - 1 = p - 1$.
2. dla każdego dzielnika d
   mamy $\phi(d)$ liczb

Tabela ilustruje także pewne fakty, które podajemy jako ...

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	**1**
3	9	**1**	3	9	1	3	9	1	3	9	1
4	3	12	9	10	**1**	4	3	12	9	10	1
5	12	8	**1**	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	**1**
7	10	5	9	11	12	6	3	8	4	2	**1**
8	12	5	**1**	8	12	5	1	8	12	5	1
9	3	**1**	9	3	1	9	3	1	9	3	1
10	9	12	3	4	**1**	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	**1**
12	**1**	12	1	12	1	12	1	12	1	12	1

... zespół twierdzeń:

Dla $a \perp m$ oraz $r = \mathrm{ord}_m(a)$ zachodzi

1. Jeśli $a^R \equiv 1 \pmod{m}$ to $r \mid R$.
   W szczególności $\boxed{r \mid \phi(m)}$.
2. Dla s i t całkowitych kongruencja
   $a^s \equiv a^t \pmod{m} \quad \Leftrightarrow \quad s \equiv t \pmod{r}$.
3. Żadne dwie liczby zbioru $a, a^2, \ldots, a^r$ nie przystają do siebie modulo m.
4. Jeżeli n jest liczbą naturalną to rząd modulo m liczby a^n jest równy $\dfrac{r}{(r,n)}$.
   W szczególności
   $\mathrm{ord}_m(a) = \mathrm{ord}_m(a^n) \quad \Leftrightarrow \quad (n, r) = 1$.

Dowód tw. **1**: jeśli $a^R \equiv 1 \pmod{m}$ to $r \mid R$. Dzielimy R przez r – mamy $R = qr + \rho$. Mamy

$$a^R = a^{qr+\rho} = (a^r)^q a^\rho \equiv a^\rho \equiv 1 \pmod{m}.$$

Kongruencja wyjściowa jest spełniona dla r będącego *najmniejszym niezerowym* wykładnikiem potęgowym;
stąd wniosek, że ρ musi być równe zeru.

Pytanie:

czy jeżeli podany jest pewien dzielnik n funkcji $\phi(m)$ to czy istnieje *zawsze* jakaś liczba a, taka, że $\mathrm{ord}_m(a) = n$?

Odpowiedź:

Nie. Na przykład dla $m = 15$ mamy $\phi(m) = 8$; wszystkie reszty względnie pierwsze z m przystają do jednej z liczb ± 1, ± 2, ± 4 i ± 7, które *wszystkie* spełniają (sprawdź!) kongruencję $x^4 \equiv 1 \pmod{15}$. Nie ma więc liczby której rząd byłby równy $n = 8$.

twierdzenie o dzielnikach liczby $\phi(p) = p - 1$

Dla modułu, będącego liczba pierwszą p, *dla każdego* dzielnika n liczby $\phi(p) = p - 1$ istnieje liczba a taka, że $\mathrm{ord}_p(a) = n$.

do jego dowodu udowodnimy najpierw twierdzenie o potęgach – twierdzenie 4:

Niech rząd pewnej liczby a modulo p (liczba pierwsza) wynosi n. Wówczas wszystkie potęgi

$$a^{r_1},\ a^{r_2},\ \ldots\ a^{r_{\phi(n)}}$$

gdzie $r_1 = 1, r_2, \ldots, r_{\phi(n)}$ to dodatnie reszty, mniejsze od i względnie pierwsze z n, mają ten sam rząd modulo p co sama liczba a.

Przykład

Z naszej tabeli wynika, że $\mathrm{ord}_{13}(2) = 12$. Reszty mniejsze i względnie pierwsze z 12 to $1, 5, 7, 11$. Z tabeli też wynika, że liczby przystające modulo 13 do takich potęg dwójki to
$2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11, \quad 2^{11} \equiv 7$. I rzeczywiście – rząd modulo 13 wszystkich tych liczb (2, 6, 11 i 7) jest równy 12 (patrz tabela (1)).

dowód twierdzenia o potęgach

$\mathrm{ord}_p(a) = n \rightarrow a$ (i n) spełnia(ją) równanie $x^n \equiv 1 \pmod{p}$.
Ale $(a^i)^n = (a^n)^i \equiv 1 \pmod{p}$ – dla każdego i i wszystkie n liczb $1, a, a^2, \ldots, a^{n-1}$ spełniają kongruencję $x^n \equiv 1 \pmod{p}$.
Co więcej – te n potęg są liczbami nie-przystającymi modulo p.
(to było tw. **3**) Inaczej mielibyśmy

$$a^i \equiv a^j \pmod{p} \quad \rightarrow \quad a^{i-j} \equiv 1 \pmod{p}$$

– a to oznaczałoby spełnienie kongruencji z wykładnikiem mniejszym od n – co jest niemożliwe.
Tak więc liczb, których rząd modulo p jest równy n, należy szukać w potęgach $1, a, \ldots, a^{n-1}$. Ale dla liczb $a_r = a^r$, gdzie wykładnik r *nie jest* względnie pierwszy z n, tzn. $NWD(n, r) = d \neq 1$ zachodzi

$$a_r{}^{n/d} = (a^n)^{r/d} \equiv 1 \pmod{p}$$

– a więc rząd tych liczb a_r jest *mniejszy* od liczby n i równy n/d.

dowód twierdzenia o potęgach, c.d.

Pozostają więc tylko $a_r = a^r$, gdzie $r \perp n$.
Jeżeli oznaczymy przez n_r rząd liczby a_r — $\mathrm{ord}_p(a_r) = n_r$ to (modulo p) mamy ${a_r}^{n_r} \equiv 1$, ale jednocześnie – ponieważ a_r jest pierwiastkiem kongruencji $x^n \equiv 1 \pmod{p}$ – $(a_r)^n = (a^n)^r \equiv 1$, skąd wynika $n_r \mid n$.
Z drugiej jednak strony, z faktu $\mathrm{ord}_p(a) = n$ oraz kongruencji

$$(a^r)^{n_r} = a^{r \cdot n_r} \equiv 1 \pmod{p}$$

wynika, że $n \mid r \cdot n_r$ – a ponieważ $r \perp n$ – to musi zachodzić $n \mid n_r$, a więc $n_r = n$. □

dowód twierdzenia o dzielnikach

Oznaczmy ν dzielników liczby $p-1$ przez

$$n_1 = 1, n_2, \ldots, n_i, \ldots, n_\nu = p-1,$$

a przez N_i – ilość liczb, których rząd modulo p jest równy n_i. Ponieważ rząd każdej liczby niepodzielnej przez p musi być którąś z liczb n_i mamy

$$N_1 + N_2 + \ldots + N_i + \ldots + N_\nu = p-1.$$

Ale z ostatnich rozważań – także twierdzenia o potęgach – wynika, że dla każdego dzielnika n_i zachodzi alternatywa – albo $N_i = 0$ (nie ma takiej liczby, której rząd wynosiłby n_i); albo – jeżeli dzielnik *jest* rzędem to liczba takich liczb $N_i = \phi(n_i)$. Z kolei, mieliśmy twierdzenie
– *suma funkcji ϕ wszystkich dzielników danej liczby jest równa tej liczbie.* To znaczy

$$\phi(n_1) + \phi(n_2) + \ldots + \phi(n_i) + \ldots + \phi(n_\nu) = p-1.$$

Porównując dwa powyższe równania mamy $N_i = \phi(n_i)$, dla każdego i. Tak więc rzeczywiście – dla każdego dzielnika n liczby $p-1$ istnieje $\phi(n)$ liczb, których rząd modulo p jest równy n.