Uniwersyteckie Kółko Matematyczne - poziom C

www.math.uni.wroc.pl/~preisner/jg

Kamil Duszenko, Jelenia Góra, 8 maja 2010 r.

1 Twierdzenia Fermata i Eulera

Jeżeli a i n są dowolnymi liczbami naturalnymi, to bardzo łatwo uzasadnić, że ciąg reszt z dzielenia liczb 1, a, a^2, a^3, a^4, ... przez n musi być okresowy, przynajmniej od pewnego miejsca. Powstaje więc naturalne pytanie: jaka jest długość tego okresu? Poniższe twierdzenia wyjaśniają tę sytuację.

Twierdzenie 1.1 (Małe tw. Fermata - wersja 1) *Niech p będzie liczbą pierwszą. Wtedy dla dowolnego całkowitego a liczba $a^p - a$ dzieli się przez p.*

Twierdzenie 1.2 (Małe tw. Fermata - wersja 2) *Niech p będzie liczbą pierwszą. Wtedy dla dowolnego całkowitego a niepodzielnego przez p liczba $a^{p-1} - 1$ dzieli się przez $p - 1$.*

Dowód. Zakładamy, że a nie dzieli się przez p; w takim razie liczby a, $2a$, $3a$, ..., $(p-2)a$, $(p-1)a$ nie dzielą się przez p oraz dają przy dzieleniu przez p parami różne reszty (gdyby ia i ja, gdzie $0 < i < j < p$, dawały te same reszty, to różnica $ja - ia = (j-i)a$ dzieliłaby się przez p, co jest niemożliwe, gdyż $0 < j - i < p$). Są to więc wszystkie reszty 1, 2, 3, ..., $p-2$, $p-1$ w pewnej kolejności, skąd iloczyny $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-2)a \cdot (p-1)a$ i $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)$ dają te same reszty z dzielenia przez p. Odejmując obie liczby i wyłączając wspólny czynnik $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)$, który nie dzieli się przez p, wnioskujemy o podzielności liczby $a^{p-1} - 1$ przez p. □

Przyglądając się powyższemu dowodowi zobaczymy, że zachowa on moc, gdy: zamiast liczby pierwszej p rozpatrzymy dowolną liczbę n, weźmiemy dowolną liczbę całkowitą a względnie pierwszą z n, zaś zamiast ciągu reszt 1, 2, 3, ..., $p-2$, $p-1$ rozważymy ciąg wszystkich reszt względnie pierwszych z n. Otrzymamy następujące wzmocnienie twierdzenia Fermata:

Definicja 1.1 (Funkcja Eulera) *Dla każdej liczby naturalnej n przez $\varphi(n)$ oznaczamy liczbę tych liczb w zbiorze $\{1, 2, 3, \ldots, n-1, n\}$, które są względnie pierwsze z liczbą n.*

Twierdzenie 1.3 (Eulera) *Niech n będzie liczbą naturalną. Wtedy dla dowolnego całkowitego a względnie pierwszego z n liczba $a^{\varphi(n)} - 1$ dzieli się przez n.*

1. Oblicz:
   (a) resztę z dzielenia liczby $2^{44} - 3^{85} + 5^{211}$ przez 43;
   (b) resztę z dzielenia liczby $2^{243} - 3^{101}$ przez 5, 7 i 35;
   (c) resztę z dzielenia liczby 2^{340} przez 341 (przyda się równość $341 \cdot 3 = 2^{10} - 1$).
2. Niech p będzie liczbą pierwszą.
   (a) Wykaż, że dla $n = p^2 - 3p + 3$ liczba $2^n - n + 1$ dzieli się przez p.
   (b) Wykaż, że dla $n = p^2 - 5p + 6$ liczba $3^n - n - 3$ dzieli się przez p, o ile $p > 3$.
3. Udowodnij, że dla każdego n
   (a) liczba $n^6 - n^2$ dzieli się przez 60;
   (b) liczba $n^{16} - n^4$ dzieli się przez $65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.
4. Udowodnij, że dla każdego n

(a) liczba $n^{n^7} - n^n$ dzieli się przez 43;

(b) liczba $n^{n^{n^{n^n}}} - n^{n^{n^n}}$ dzieli się przez liczbę pierwszą 547.

5. Udowodnij, że dla dowolnej liczby naturalnej n istnieją liczby naturalne $r > s$ o następującej własności: Dla każdego całkowitego a liczba $a^r - a^s$ dzieli się przez n.

6. Wykaż, że każda liczba naturalna niepodzielna przez 2 ani przez 5 posiada wielokrotność o zapisie dziesiętnym postaci $101010\ldots01010101$.

7. Wykaż, że dla każdej liczby naturalnej n liczba $n^{561} - n$ dzieli się przez $561 = 3 \cdot 11 \cdot 17$. (Liczby złożone o takiej własności nazywają się *liczbami Carmichaela*; 561 jest najmniejszą z nich).

8. Przypuśćmy, że dla pewnego k liczby $6k + 1$, $12k + 1$, $18k + 1$ są pierwsze. Udowodnij, że iloczyn tych trzech liczb jest liczbą Carmichaela.

9. Dokończ i uzasadnij następujące kryterium: liczbą Carmichaela jest każda liczba naturalna n, która nie dzieli się przez kwadrat liczby pierwszej i taka, że jeśli p jest dzielnikiem pierwszym n, to ... jest dzielnikiem ....

10. Niech p będzie liczbą pierwszą i niech k będzie liczbą naturalną względnie pierwszą z $p - 1$. Udowodnij, że reszty z dzielenia liczb 1^k, 2^k, 3^k, ..., $(p-2)^k$, $(p-1)^k$ przez p są z dokładnością do kolejności równe 1, 2, 3, ..., $p - 2$, $p - 1$. Jak uogólnić ten wynik na przypadek, gdy p nie jest liczbą pierwszą?

11. Niech $p > 2$ będzie liczbą pierwszą dającą resztę 2 z dzielenia przez 3. Udowodnij, że iloczyn $(2^2 + 2 + 1)(3^2 + 3 + 1)(4^2 + 4 + 1) \ldots [(p - 1)^2 + (p - 1) + 1]$ daje resztę 1 z dzielenia przez p.

12. Niech $p > 3$ będzie liczbą pierwszą. Wykaż, że liczba $2^{p-2} + 3^{p-2} + 6^{p-2}$ daje resztę 1 z dzielenia przez p.

13. Wykaż, że z ciągu $2^2 - 3$, $2^3 - 3$, $2^4 - 3$, $2^5 - 3$, ... można wybrać nieskończenie wiele liczb, z których dowolne dwie są względnie pierwsze.

14. Wykaż, że dowolny dzielnik pierwszy liczby $2^p - 1$, gdzie p jest liczbą pierwszą, daje resztę 1 z dzielenia przez p.

15. Wykaż, że dowolny dzielnik pierwszy liczby $2^{2^n} + 1$ daje resztę 1 z dzielenia przez 2^{n+1}.

16. Udowodnij, że dla żadnego naturalnego $n > 1$ liczba $2^n - 1$ nie dzieli się przez n.

17. Niech p będzie nieparzystą liczbą pierwszą. Udowodnij, że dowolny dzielnik pierwszy liczby $\frac{1}{3}(4^p - 2^p + 1)$ daje resztę 1 z dzielenia przez 6.

18. Niech $W(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ będzie wielomianem o współczynnikach całkowitych. Przypuśćmy, że dla każdej liczby naturalnej n liczba $2^n - 1$ dzieli się przez $W(n)$. Wykaż, że wówczas dla każdego naturalnego n mamy $W(n) = \pm 1$.