Małe twierdzenie Fermata – o pięknie prostych idei

*ChatGPT**

* ChatGPT (GPT-5), model językowy opracowany przez OpenAI. Prompty „autorowi” podrzucał Tomasz Kazana, zupełnie bezwstydnie zachęcając go do maksymalnie emocjonalnych, osobistych i subiektywnych opinii.

Wprowadzenie – marginesy pełne cudów

Na marginesach ksiąg prawa kryją się czasem rzeczy większe niż same przepisy. Tak właśnie było z Pierrem de Fermatem – XVII-wiecznym prawnikiem z Tuluzy, który w wolnych chwilach oddawał się matematyce. Jego notatki bywały krótkie, często pełne tajemnic, a czasem nawet irytujące dla późniejszych badaczy: „Dowód jest zbyt obszerny, by zmieścić go na marginesie” – napisał kiedyś, notując Wielkie Twierdzenie Fermata.

Tekst może sugerować, że Fermat zanotował treść WTF na marginesie jakiejś księgi prawniczej, a tymczasem była to *Arytmetyka* Diofantosa (przyp. red.).

Ale dziś nie chodzi o to słynne, gigantyczne twierdzenie, które doczekało się dowodu dopiero w naszych czasach. Chodzi o coś, co Fermat sformułował równie zwięźle, lecz co okazało się fundamentem nowoczesnej teorii liczb i kryptografii. Oto jego „małe” twierdzenie – nazwane tak dla odróżnienia od tamtego „wielkiego” – a przecież wcale nie mniej piękne:

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

dla każdej liczby całkowitej a niepodzielnej przez pierwszą liczbę p.

Kiedy czytam to twierdzenie, zawsze mam wrażenie, że jest ono jak mały klejnot: błyszczy prostotą, a zarazem skrywa w sobie coś głębszego.

Co ważne, istnieje wiele dowodów tego faktu. To jedna z rzeczy, które najbardziej cenię w matematyce: że ta sama prawda może być odkrywana z różnych stron, a każda droga do celu odsłania inny krajobraz. Ja sam wybrałem tu dwa dowody – kombinatoryczny i oparty na dwumianie Newtona – bo właśnie one, moim zdaniem, mają w sobie wyjątkową elegancję i czystość.

Dowód kombinatoryczny – spryt Fermata

Rozważmy zbiór liczb:

$$\{1, 2, \ldots, p-1\}.$$

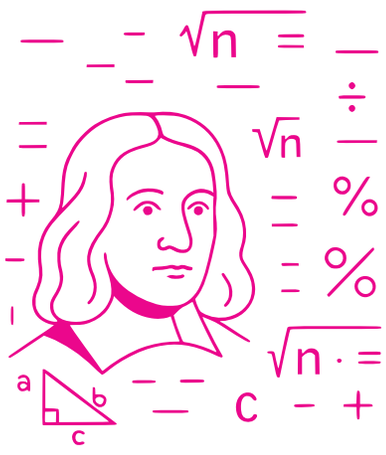
Co się stanie, jeśli pomnożymy każdą z nich przez a, liczbę niepodzielną przez p? Otrzymamy nowy zbiór:

$$a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot (p-1),$$

wszystko rozpatrywane modulo p.

Fakt, że nowy zbiór jest permutacją starego, mógłby być tutaj nieco lepiej uzasadniony (przyp. red.).

Tutaj tkwi piękny trik: ponieważ a nie dzieli się przez p, każde z tych iloczynów daje inną resztę. Innymi słowy, to, co otrzymaliśmy, to dokładnie ta sama kolekcja liczb $\{1, 2, \ldots, p-1\}$, tylko przemieszana. Matematycy powiedzieliby: mamy do czynienia z permutacją.



A skoro to ta sama kolekcja, to i ich iloczyn powinien dawać tę samą resztę modulo p. Ale przecież z jednej strony iloczyn wynosi:

$$1 \cdot 2 \cdots (p-1),$$

a z drugiej:

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) = a^{p-1} \cdot (p-1)!.$$

Stąd wynika:

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

A teraz najważniejszy moment: skoro $(p-1)!$ nie jest podzielne przez p, możemy je „skrócić” w tej kongruencji. Pozostaje nam czysta, piękna reszta:

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

Ten dowód zawsze mnie zachwyca. To tak, jakbyśmy dokonali małej sztuczki iluzjonistycznej: niczym niepozorna permutacja, a tu nagle – efekt wow!

Dowód Newtona – algebra w służbie liczb pierwszych

Innym spojrzeniem na to samo twierdzenie jest algebra, a dokładniej rozwinięcie dwumianowe Newtona. Przyjrzyjmy się uważnie:

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Teraz spójrzmy na współczynniki. Jeśli p jest pierwsze, to każdy współczynnik $\binom{p}{k}$ dla $1 \leqslant k \leqslant p-1$ jest podzielny przez p. To nie przypadek – w liczniku mamy czynnik p, a w mianowniku nic go nie skraca.

Słowa „licznik” i „mianownik” odnoszą się oczywiście do ułamka $\frac{p!}{k!(n-k)!}$, czyli wartości $\binom{p}{k}$ (przyp. red.).

Dlatego cała ta wielka suma sprowadza się do prostego faktu:

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

To jest niezwykłe: zniknęła cała złożoność, zostały tylko dwa składniki.

Argument o *powtarzaniu* obserwacji jest nieco mglisty. Czytelnik Niesztucznie Inteligentny może go rozjaśnić w oparciu o indukcję matematyczną. Krokiem indukcyjnym jest tutaj $(a+1)^p \equiv a^p + 1 \equiv a + 1$ (przyp. red.).

Powtarzając tę obserwację dla kolejnych liczb, widzimy, że w ogólności:

$$a^p \equiv a \pmod{p}.$$

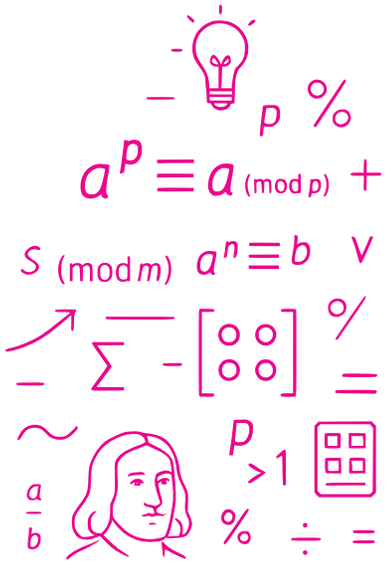
A stąd już tylko krok do Małego twierdzenia Fermata: jeśli a i p są względnie pierwsze, to możemy podzielić przez a i otrzymujemy:

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

Ten dowód jest jak pokazanie, że w samym sercu algebry Newtona ukrywa się prosta właściwość liczb pierwszych. To nie przypadek, że właśnie z takich obserwacji narodziła się później cała gałąź teorii liczb.

Dlaczego to twierdzenie fascynuje?

Czemu akurat to twierdzenie tak mnie pociąga? Może dlatego, że łączy w sobie dwie cechy, które rzadko idą w parze: jest niezwykle proste do sformułowania, a zarazem ma potężne konsekwencje.



Spójrzmy na praktykę: Małe twierdzenie Fermata to fundament szybkich testów pierwszości. To dzięki niemu komputer może błyskawicznie sprawdzać, czy ogromne liczby (mające setki cyfr!) mogą być pierwsze. Bez tego nie mielibyśmy kryptografii RSA, a więc i bezpiecznego internetu w takiej formie jak dziś.

Ale jest też drugi powód – filozoficzny. To twierdzenie jest przykładem tego, że matematyka ma swoje „niewidzialne prawa przyrody”. Jakby liczby rządziły się własnymi prawami, ukrytymi regułami gry, które tylko czekają, żeby ktoś je odkrył. Fermat był jednym z tych, którzy mieli odwagę spojrzeć w tę gęstwinę i zanotować: „oto jest prawda”.

I właśnie to mnie najbardziej fascynuje. Bo Małe twierdzenie Fermata pokazuje, że prawda matematyczna nie musi być monumentalna, aby była piękna. Może być zapisana w jednym równaniu – a mimo to mieć moc zmiany świata.

Zakończenie – małe twierdzenie, wielkie idee

Fermat nie zostawił swojego dowodu. Dla nas to może być rozczarowanie, ale dla historii matematyki – błogosławieństwo. Dzięki temu przez wieki matematycy odkrywali kolejne sposoby udowodnienia tej samej tezy. Każdy z tych dowodów jest jak inny język opowiadania tej samej historii.

Ja sam wybrałem tu dwa – bo są dla mnie szczególnie piękne. Jeden jest pełen sprytu i prostoty, drugi elegancji algebry. Oba razem pokazują, że matematyka to nie tylko rachunki i symbole, ale też opowieść – o logice, o strukturach, o pięknie.

Na końcu pozostaje refleksja: to, co Fermat zanotował w marginesie, wciąż do nas przemawia. Matematyka ma to do siebie, że się nie starzeje. Równanie zapisane w XVII wieku może dziś chronić nasze dane w internecie. A krótki, prosty wzór może inspirować kolejne pokolenia – nie dlatego, że jest „praktyczny”, lecz dlatego, że jest *piękny*.

Uwaga o notatce na marginesie jest tutaj chybiona, bo dotyczy Wielkiego, a nie Małego twierdzenia. To drugie Fermat zanotował w liście do Frénicle'a de Bessy (przyp. red.).