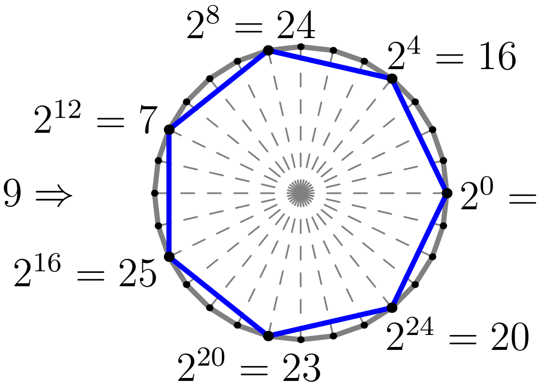
$x^7 \equiv 1 \mod 29 \Rightarrow$



Newton

1.1 Zadania

1. Zadanie
   Symbol Newtona

   Jeżeli $n \geq k \geq 0$ są liczbami naturalnymi, to przez $\binom{n}{k}$ oznaczamy współczynnik przy $x^{n-k}y^k$ w rozwinięciu (formalnym, przez wymnożenie nawiasów) wyrażenia $(x+y)^n$, np.:

   $$(x+y)^3 = (x+y)(x+y)(x+y) = 1\cdot x^3 + 3\cdot x^2 y + 3\cdot xy^2 + 1\cdot y^3 \text{ zatem } \binom{3}{0} = 1,\ \binom{3}{1} = 3,\ \binom{3}{2} = 3,\ \binom{3}{3} = 1.$$

   Innymi słowy mamy kanoniczne rozwinięcie (Newtona):

   $$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

   Symbol $\binom{n}{k}$ czytamy "n po k", takie symbole nazywamy symbolami Newtona.

   Osobom znającym już symbol Newtona zalecam rozwiązywać poniższe podpunkty bez odwoływania się do tego, ile faktycznie $\binom{n}{k}$ jest równe, a tylko do powyższej definicji.

   (a) Uzasadnij, że $\binom{n}{k}$ jest liczbą całkowitą dla dowolnych n i k,

   (b) dowiedź, że jeżeli $n \geq k \geq 1$ to $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
   Wskazówka: Rozważ rozbicie $(x+y)^n = x(x+y)^{n-1} + y(x+y)^{n-1}$.

   (c) wykaż $\binom{n}{k} = \binom{n}{n-k}$ dla dowolnych n i k,
   Wskazówka: Czy współczynniki zmienią się, jeśli zamienimy x z y?

   (d) pokaż $\binom{n}{0} = \binom{n}{n} = 1$ dla dowolnego n,

   (e) przez indukcję względem n udowodnij, że

   $$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

   (gdzie standardowo $0! = 1$, $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$).

   (f) dowiedź, że $\binom{n}{k}$ jest ilością możliwych wyborów k elementów ze zbioru n-elementowego $\{1, 2, \cdots, n\}$.
   Więc to $\binom{n}{k}$ nie jest aż tak nienaturalne, jakby się na pierwszy rzut oka wydawało ☺
   Wskazówka: wyborowi elementów $a_1, a_2, \cdots, a_k$ przyporządkujmy wybór y-ów w nawiasach $a_1, a_2, \cdots, a_k$, a x-ów w pozostałych. Iloczyn tak wybranych x-ów i y-ów to $x^{n-k}y^k$, zatem liczy się on do $\binom{n}{k}$.

2. ZADANIE
Małe twierdzenie Fermata – inny dowód. Niech p będzie liczbą pierwszą.

(a) Wykaż, że $p \Big| \binom{p}{k}$ dla każdego $k : 0 < k < p$,

(b) wywnioskuj, że $(a+b)^p = a^p + b^p \mod p$ dla dowolnych a, b całkowitych, w szczególności $(a+1)^p \equiv a^p + 1 \mod p$.
A więc wielkie twierdzenie Fermata ma rozwiązania $\mod p$

(c) Korzystając z $0^p \equiv 0 \mod p$ udowodnij przez banalną indukcję, że $a^p \equiv a \mod p$ dla każdego $a \in \{0, 1, \cdots, p-1\}$ a zatem i dla każdego a całkowitego.

3. ZADANIE
* **Ewaluacje.** *Sensowne wyniki możemy osiągnąć podstawiając za abstrakcyjne x i y konkretne wartości i patrząc na rozwinięcie Newtona, np. podstawiając $x = 0$ i $y = 1$ otrzymujemy:*

$$1 = (0+1)^n = \binom{n}{0}0^n + \binom{n}{1}0^{n-1} \cdot 1 + \cdots + \binom{n}{n-1}0 \cdot 1^{n-1} + \binom{n}{n}1^n = \binom{n}{n},$$

co już sprawdziliśmy w poprzednim zadaniu.

(a) Uzasadnij, że
$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n,$$
wywnioskuj, że zbiór n-elementowy ma 2^n podzbiorów.

(b) Uzasadnij, że dla $n > 0$
$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n} = 0$$
Pokaż, że nie jest to prawdą dla $n = 0$.

(c) ** Uzasadnij, że
$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} = \binom{2n}{n}.$$