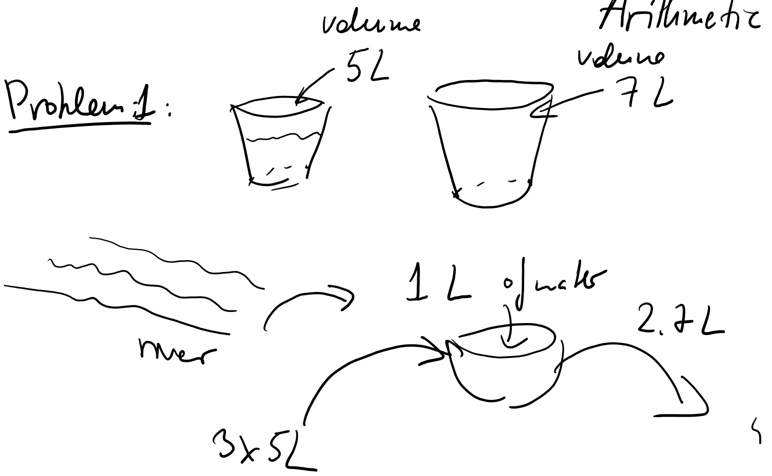
Arithmetic (number theory)

Problem 1:



$3.5 - 2.7 = 1$

① $n \nmid 2^n - 1$ for any $n \in \mathbb{N}$
② $n \nmid 2^n + 2$ for any odd > 1 $n \in \mathbb{N}$
③ $10^{10^{10^n}} + 10^{10^n} + 10^n - 1$ is not prime for any n.

Def. a, b, $\underline{gcd}(a,b) = d$ (greatest common divisor → max $\underline{d}$: $d \mid a$, $d \mid b$)

e.g. $gcd(12, 18) = 6$

$\Downarrow$

there exist $x, y \in \mathbb{Z}$: $ax + by = d$

division with remainder, say $a > b \Rightarrow a = q \cdot b + r$, $q \in \mathbb{Z}$, $0 \le r < b$

$gcd(a,b) = gcd(b, r)$

$(qb + r)x + by = d$

$b(qx + y) + rx = d$

by induction: solve $b \cdot x' + r \cdot y' = d \Rightarrow \underline{x = y'}$, $qx + y = x' \Rightarrow y = \underline{x' - qx}$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ← unique prime numbers decomposition for every integer.

(prime number → no other divisors except 1, and itself)

2, 3, 5, 7, 11, 13, ... → infinitely many.

$12 = 2^2 \cdot 3$

$2020 = 2^2 \cdot 5 \cdot \underline{101}$

if $p \cdot q = n$

$p \le q \Rightarrow p \le \sqrt{n}$

check for prime divisors $\le \sqrt{n}$

check $2, 3, 5, 7 \mid 101$?

Modular arithmetic

$x \equiv y \pmod{n} \iff n \mid x-y$

$z \equiv w \pmod{n} \Rightarrow x+z \equiv y+w \pmod{n}$

$\underline{\underline{x.z}} \equiv z.y \pmod{n} \equiv \underline{\underline{y.w}} \pmod{n}$

$(\Leftarrow n \mid (x-y).z)$

$9 \mid 10^k - 1$ $\quad k\begin{cases}10 \equiv 1 \pmod 9\\ 10 \equiv 1 \\ \vdots \\ 10 \equiv 1 \pmod 9\end{cases} \Rightarrow 10^k \equiv 1 \pmod 9$

ex. $4^{3x+1} + 2^{3x+1} + 1 \equiv ? \pmod 7$

$4^{3x+1} = (4^3)^x \cdot 4 \equiv 1^x \cdot 4 \pmod 7$

$2^{3x+1} = (2^3)^x \cdot 2 \equiv 1^x \cdot 2 \pmod 7$

$\equiv 4+2+1 = 0$

Putnam 2020, A1. How many integers N satisfy the following 3 conditions...

(1) $2020 \mid N$

(2) N has at most 2020 decimal digit

(3) $N = 1\ldots1\,0\ldots0$

$2020 = 2 \cdot 10 \cdot 101$

$101 \cdot 11 = 1111 \rightarrow$ if $N = 1111\,1111\ldots1111\,\underbrace{0\ldots0}_{\geq 2}$

$1111 \cdot 10^{\cdots} + 1111 \cdot 10^{\cdots}$

When does $101 \mid \underbrace{11\ldots1}_{m} = \dfrac{\overset{n}{99\ldots9}}{9} = \dfrac{10^m - 1}{9}$?

which m

$10^m \overset{?}{\equiv} 1 \pmod{101}$

$10 \equiv 10 \pmod{101}$

$10^2 \equiv 100 \equiv -1 \pmod{101}$

$\Rightarrow$ if $m = 4q + r \quad 0 \leq r \leq 3$

$\Rightarrow 10^m \equiv (10^4)^q \cdot 10^r \equiv 10^r \pmod{101}$

$10 \equiv 10 \pmod{101}$

$10^2 \equiv 100 \equiv -1 \pmod{101}$

$10^3 \equiv -10 \pmod{101}$

$10^4 \equiv (10^2)^2 \equiv 1 \pmod{101}$

min power, $10^4 \equiv 1 \pmod{101}$

$\Rightarrow$ U

$\Rightarrow 10^m \equiv (10^4)^q \cdot 10^r \equiv 10^r \pmod{101}$

$1 \Leftrightarrow r=0$

10

can prove: if $10^m \equiv 1 \pmod{101}$

$\Rightarrow 4 \mid m$

Theorem: $a, n \in \mathbb{Z}$, $\gcd(a,n) = 1 \Rightarrow$

1) $\exists\, m < n$, s.t. $a^m \equiv 1 \pmod n$

$\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ ← units → group

$a^1, a^2, a^3, \dots, a^{n-1} \pmod n$

$\{1, 2, \dots, n-1\}$ ← coprime with n

Pigeonhole: either 1-to-1, so $a^m \equiv 1 \pmod n$ ✓

or if not $n-1$ elem → $n-2$ res. classes $\Rightarrow a^i \equiv a^j \pmod n$

$i > j$

$\Rightarrow \cancel{a^j}\,(a^{i-j}-1) \equiv 0 \pmod n$

$\Rightarrow a^{i-j} \equiv 1 \pmod n$, $i-j = m$

2) Let m ← order of a in $(\mathbb{Z}/n\mathbb{Z})^*$: min s.t. $a^m \equiv 1 \pmod n$.

If $a^k \equiv 1 \pmod n \Rightarrow m \mid k$

$k > m$, $k = m \cdot q + r$, $0 \le r < m$

$\Rightarrow 1 \equiv a^k \equiv a^{mq+r} \equiv (a^m)^q \cdot a^r \equiv a^r \pmod n$

$a^m \equiv 1 \pmod n$

$\Rightarrow a^r \equiv 1 \pmod n$, but $r < m \Rightarrow r = 0 \to k = m \cdot q$.

Euler's totient function:

$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$, $\alpha_i \in \mathbb{N}_{>0}$

$\phi(n) := \#\{ m \mid 1 \le m \le n \mid \gcd(m, n) = 1 \}$.

If $n = p \rightarrow \phi(p) = p-1$

$n = p^2$ $\quad \gcd(m, n) = 1$ or p or p^2 ($m \le n$)

? $\quad\quad$ $m = n$!

$1, 2, \ldots, p^2$

$px \le p^2 \Leftrightarrow x < p$

$1 \cdot p, 2p, \ldots (p-1)p$) $\underline{p-1}$ such numbers.

$$\Rightarrow \phi(p^2) = p^2 - 1 - (p-1) = p^2 - p = p(p-1)$$

$$\phi(p^k) = p^k - p^{k-1}$$

In $\underline{\text{general}}$: $\underline{\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)}$

(proof by Inclusion-Exclusion).

$\underline{\text{Euler (Fermat's little theorem)}}$: if $\gcd(a, n) = 1 \Rightarrow \underline{a^{\phi(n)} \equiv 1 \pmod n}$

$\phi(12) = \phi(2^2 \cdot 3) = 2(2-1)\cdot(3-1) = 4 \quad \Rightarrow$ e.g. $7^4 \equiv 1 \pmod{12}$

$5^4 \equiv 1 \pmod{12}$

$11^4 \equiv 1 \pmod{12}$

$\underline{\text{Proof.}}$ $\quad S = \{a_1, a_2, \ldots, a_{\phi(n)}\} \leftarrow$ res. classes mod n, rel. prime to n,

e.g. $n = 12 \rightarrow \{1, 5, 7, 11\}$

a; $\gcd(a, n) = 1$ $\quad a \cdot S = \{a a_1, a a_2, \ldots, a a_{\phi(n)}\} \pmod n$

$\quad\quad\quad\quad \shortparallel$ $\quad$ distinct $\quad a a_i - a a_j = a(a_i - a_j) \not\equiv 0 \pmod n$

$\quad\quad\quad\quad S$ $\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \ne 0$

$$\Rightarrow \prod_{i=1}^{\phi(n)} (a a_i) \equiv \prod_{i=1}^{\phi(n)} a_i \pmod n$$

$\quad\quad \shortparallel$

$$a^{\phi(n)} \cancel{\prod a_i} \equiv \cancel{\prod a_i} \pmod n$$

$$\cancel{a^{\phi(n)} \prod a_i} \equiv \cancel{\prod a_i} \pmod n$$

$$\rightarrow \quad a^{\phi(n)} \equiv 1 \pmod n$$

Pr. $n \nmid 2^n - 1$

Suppose:

$n \mid 2^n - 1$

$n \rightarrow$ odd

case 1

$n = p \qquad p \mid 2^{p-1} - 1$

$$2^{p-1} \equiv 1 \pmod p$$
$$2^p \equiv 1 \pmod p$$
$$2^p \equiv 2^{p-1} \pmod p$$
$$\rightarrow 2^{p-(p-1)} \equiv 1 \pmod p$$
$$2^1 \equiv 1 \pmod p \rightarrow \text{no}.$$

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $p_1 < p_2 < \cdots < p_k$ ($p_1 = p$)

$\Rightarrow \quad p \mid n \mid 2^n - 1 \Rightarrow p \mid 2^n - 1$, $\quad p \mid 2^{p-1} - 1$, let $2^m \equiv 1 \pmod p$ (order mod p)

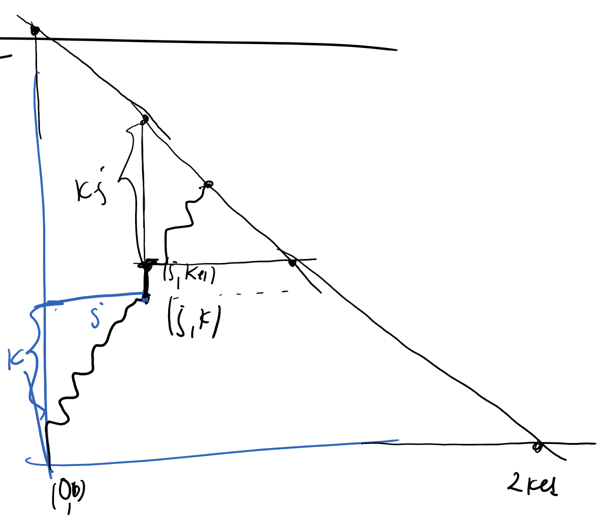
$m \mid n \qquad m \mid p_1 - 1$

only prime divisors of $m \in \{p_1, p_2, \dots, p_k\}$, $m = p_1^{\beta_1} \cdots p_k^{\beta_k} \nmid p_1 - 1$ (all prime div. $< p_1$)

$\Rightarrow$ Contradiction $\rightarrow$ no.

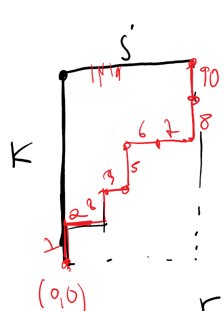
$n \nmid 2^n + 2$

A2: $\displaystyle\sum_{j=0}^{k} 2^{k-j} \binom{k+j}{j}$

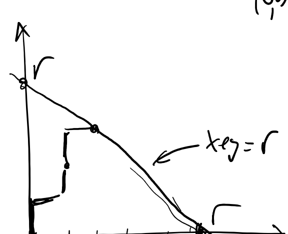


j horizontal

k vertical



$2^r =$



Paths codes with r steps, each step 1 or –

lattice codes with r steps, each step | or —