4 and 5 $x^2 \equiv -1 \pmod p$ has a solution iff $(p=2)$ or $p \equiv 1 \pmod 4$

$\Rightarrow$ $x^2 \equiv -1 \pmod p$, $2 \mid p-1$ $\quad \alpha = \frac{p-1}{2}$ $\Rightarrow (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$

$\pmod p$ $1 \equiv x^{p-1}$ $\qquad +1$, $4 \mid p-1$ $\qquad -1$, $4 \nmid p-1$ $\to$ impossible.

$\Leftarrow$ $p \equiv 1 \pmod 4$

for every a, $p \nmid a$

$\Rightarrow \exists\, b : ab \equiv 1 \pmod p$

(e.g. $b = a^{p-2}$)

$\Rightarrow b = a^{-1}$ unique. $\quad ab_1 \equiv 1$, $ab_2 \equiv 1$ $-$ $\quad p \mid a(b_1 - b_2) \Rightarrow p \mid b_1 - b_2$

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

$a, b \in \{1, 2, 3, \ldots, p-2, p-1\}$

$\{2, \frac{p+1}{2}\}\ \{3, \frac{p}{?}\} \ldots$

pairs. a, a^{-1}

$a \neq a^{-1}$ unless $a = 1$ or $p-1$

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

$\Rightarrow a^2 \equiv 1 \pmod p$

$p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ or $p \mid a+1 \Rightarrow a = 1$ or $p-1$

$1.2 \ldots (p-1) = \prod_a (a \cdot a^{-1}) \cdot 1 \cdot (p-1) = -1 \pmod p$

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

$\Rightarrow$ $\boxed{\text{Wilson's theorem: } (p-1)! \equiv -1 \pmod p}$

Now, let $p \equiv 1 \pmod 4$ $\to$ find x : $x^2 \equiv -1 \pmod p$

$p-1 = 4m$

$x = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$ $\quad \Rightarrow \quad x \equiv (-1)^{\frac{p-1}{2}} \cdot y \pmod p$, $\frac{p-1}{2} \to$ even.

(-1) ||| $\quad$ |||

$(p-1)(p-2) \ldots \left(\frac{p+1}{2}\right) = y$ $\pmod p$ $\quad \Rightarrow \quad \boxed{x \equiv y \pmod p}$.

$x^2 \equiv x \cdot y = 1 \cdot 2 \ldots (p-1) \equiv -1 \pmod p$

Wilson's th.

Wilson's th.

$\Rightarrow \underline{x^2 \equiv -1 \pmod{p}}$

Infinitely many primes $\equiv 1 \pmod 4$

$p_1, p_2, \dots, p_n \rightarrow$ all the primes $\equiv 1 \pmod 4$

$\underline{N = \underbrace{4p_1^2 \cdots p_n^2}_{(2p_1 \cdots p_n)^2,\ x} + 1} \rightarrow$ it is not divisible by any of $\underline{p_1, \dots, p_n}$

(caveat: it could have all primes $\equiv 3 \pmod 4$ divisors)

$(4n_1 + 3)(4n_2 + 3) \equiv 1 \pmod 4$

Let $q \mid N = x^2 + 1$, $\xRightarrow{\text{by th. 4}}$ $q \equiv 1 \pmod 4$, $q \neq p_1 \dots p_n$

prime.

$\rightarrow$ new prime $\equiv 1 \pmod 4$ $\rightarrow$ contradiction.

Problem: does there exist a positive integer k, s.t.

$k \cdot 2^n + 1$ $\rightarrow$ is composite for every $n \in \mathbb{N}$.

$2^x + 3 = z^3$ $\leftarrow$ does this have a solution with $x, z \in \mathbb{N}$

Euler's totient function $\phi(n) = \# \underbrace{\{ m < n,\ \gcd(m,n) = 1 \}}_{\Phi(n)}$

$\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \underline{p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)}$

---

1 $\boxed{\sum_{k \mid n} \phi(k) = n}$

$n = p$, $\phi(p) = p - 1$

$\phi(1) + \phi(p) = 1 + p - 1 = p$

$n = p^2$

$\phi(1) + \phi(p) + \phi(p^2) = 1 + p - 1 + p(p-1) = p^2 = n$

Proof: Let $m \le n$, $d = \gcd(m,n)$

$m = d \cdot m_1$ $\quad \gcd(m_1, n_1) = 1$

$n = d \cdot n_1$ $\quad$ Let $n_1 \mid n$, $m_1 \in \Phi(n_1)$

$$\{1,2,\dots,n\} \Longleftrightarrow \bigcup_{d \mid n} \Phi\left(\overset{n_1}{\overset{\shortparallel}{\frac{n}{d}}}\right) \longleftarrow \sum_{d \mid n} \phi\left(\overset{k}{\frac{n}{d}}\right)$$

m

$\Longleftrightarrow$ let m_1: $\gcd(m_1, k) = 1$

$$m = \overset{d}{\frac{n}{k}} \cdot m_1 \longleftarrow$$

$$n = \sum_{k \mid n} \phi(k)$$

$\gcd(a,d) = 1$

$1 < a,\ a+d,\ a+2d,\ a+3d,\ \dots,\ a+nd,\ \dots$

There is an infinite subset $\{ \underbrace{a + n_i d}_{\substack{\shortparallel \\ p_1^{\alpha_1} \cdots p_k^{\alpha_k}}} \mid i = 1, 2, \dots \}$ $\leftarrow$ same prime factors.

$d = 3$

$1,\ 4,\ 7,\ 10,\ 13,\ 16,\ \dots$

$a^{\phi(d)} \equiv 1 \pmod d \ \rightarrow\ a^{k\phi(d)} \equiv 1 \pmod d$

$\rightarrow a^{k\phi(d)} = 1 + m_k d$

$\rightarrow a^{k\phi(d)+1} = a + \underbrace{a m_k}_{n_k} d$

$$\rightarrow S = \{ \underbrace{a^{k\phi(d)+1}}_{a + n_k d} \mid k = 1, 2, \dots \}$$

Green-Tao theorem: The prime numbers $2, 3, 5, \dots$ contain arithmetic progressions of any length.

for any k: can find a, d $\quad a,\ a+d,\ a+2d,\ \dots,\ a+kd$

prime numbers.

If p - prime $\rightarrow$ $a^{p-1} \equiv 1 \pmod p$

Chinese remainder theorem.

$n_1, n_2 \dots n_k \leftarrow \gcd(n_i, n_j) = 1 \quad \forall i \neq j$,

any set of numbers $b_1 \dots b_k$

$\Rightarrow$ $x \equiv b_1 \pmod{n_1}$
$\vdots$
$x \equiv b_{k-1} \pmod{n_{k-1}}$
$x \equiv b_k \pmod{n_k}$ has a solution

$x \equiv B \pmod{n_1 n_2 \dots n_{k-1}}$
$x \equiv b_k \pmod{n_k}$

proof is by induction on k

$k = 2$:

$x \equiv b_1 \pmod{n_1}$
$x \equiv b_2 \pmod{n_2}$

use $pn_1 + qn_2 = 1$

$$\boxed{\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \end{aligned}} \longleftrightarrow \begin{aligned} x+1 &\equiv 0 \pmod 2 \\ &\equiv 0 \pmod 3 \end{aligned} \Leftrightarrow x+1 \equiv 0 \pmod 6$$

$x \equiv 4 \pmod 5$

$x \equiv 4 \pmod 5$
$x+1 \equiv 0 \pmod 5$

$\Rightarrow x+1 \equiv 0 \pmod{30}$

$\boxed{x = 29}$

$n = 1\,000\,000$ consecutive integers, each divisible by some p^2, p - prime.

$x, \; x+1, \; x+2, \; \dots, \; x+n-1$

$p_1^2 \quad p_2^2 \quad p_3^2 \quad p_n^2$

$p_k^2 \mid x+k-1 \longrightarrow$

$x \equiv 0 \pmod{p_1^2}$
$\vdots$
$x \equiv -k+1 \pmod{p_k^2}$
$\vdots$
$x \equiv -n+1 \pmod{p_n^2}$

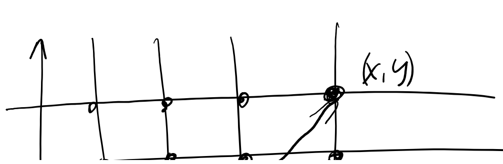
can find an x

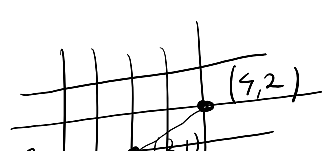
$(x, y) \in \mathbb{Z}^2$ is visible if $\boxed{\gcd(x, y) = 1}$

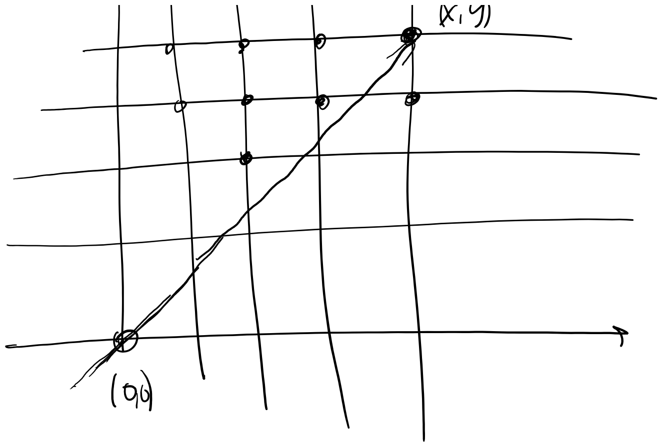
(otherwise $\frac{x}{y} = \frac{p}{q}$

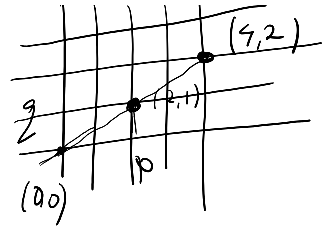
if $\gcd(x, y) = d$
$x = dx_1, \; y = dy_1$

$\Rightarrow \quad \rightarrow (x, y)$



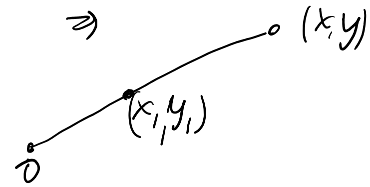




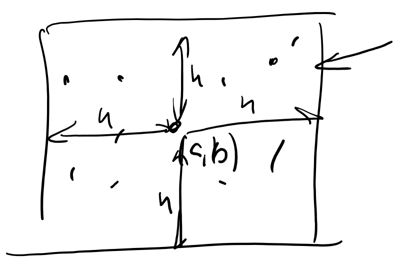


$x = dx_1, \quad y = dy_1$

$\Rightarrow$



Problem: given n, can we find a point (a,b), s.t.



all of these points are invisible.