Last time: Quadratic Reciprocity

p, q odd primes $\quad p \neq q$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

We saw some problems too!

→ Determine whether 5 is a square mod 101.

→ Find all primes p such that 3 is a square mod p.

Let's discuss more applications.

<u>Lemma:</u> Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a non constant polynomial with $a_i \in \mathbb{Z}$. Then there are infinitely many primes among factors of $f(n)$ for $n \in \mathbb{Z}$.

<u>Pf:</u> Suppose $p_1, \ldots, p_t$ are finitely many primes dividing $f(n_1), f(n_2), \ldots, f(n_t)$

$$P = p_1 \cdots p_t$$

$p_1, p_2, \ldots p_t$ $\qquad$ $p_i \mid f(m_i)$

$P = p_1 p_2 \cdots p_t$

$f(x) = a_0 + a_1 x + \cdots + a_d x^d$

$a_0 = 0$ $\qquad$ $f(0) = 0$ $\qquad$ Every prime divides $f(0)$.

$a_0 \neq 0$ $\qquad$ $\dfrac{f(k a_0 P)}{a_0} = \dfrac{1}{a_0}\left(a_0 + a_1 k a_0 P + \cdots + a_d k^d a_0^d P^d\right)$

$= 1 + a_1 k P + a_2 k^2 a_0 P^2 + \cdots + a_d k^d a_0^{d-1} P^d$

1. If a prime $q \mid RHS$ then $q \nmid P$.

2. Think of RHS as a polynomial in k, as k gets large there is a prime divisor of $RHS = \dfrac{f(kq_0P)}{q_0} \implies$

it must divide $f(kq_0P)$.

Some Corollaries

→ Let $a \neq 0 \in \mathbb{Z}$. There are infinitely many primes p such that $\left(\frac{a}{p}\right) = 1$.

Proof: Take $f(x) = x^2 - a$.

There are infinitely many primes p such that $p \mid f(n)$ as n varies in $\mathbb{Z}$.

$$n^2 \equiv a \pmod{p}$$

$$x^2 \equiv a \pmod p \implies \left(\frac{a}{p}\right) = 0$$

$$\text{or } \left(\frac{a}{p}\right) = 1$$

$\implies$ There are infinitely many Primes p s.t $\left(\frac{a}{p}\right) = 1$.

$\rightarrow$ There are infinitely many Primes $p \equiv 1 \pmod 4$.

Pf: Take $a = -1$

→ There are infinitely many primes $p \equiv 1 \pmod{3}$

Pf: Take $a = -3$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}}$$

$$= \left(\frac{p}{3}\right)$$

$\left(p/3\right) = 1 \iff p \equiv 1 \pmod{3}$

Jacobi Symbol

(Generalization of Legendre Symbol)

If $n = 3^{e_3} 5^{e_5} 7^{e_7} \cdots$

$a \in \mathbb{Z}$ $$\left(\frac{a}{n}\right) = \left(\frac{a}{3}\right)^{e_3} \left(\frac{a}{5}\right)^{e_5} \left(\frac{a}{7}\right)^{e_7} \cdots$$

The following properties are satisfied by Jacobi Symbol.

i) If $a \equiv b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

ii) $$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$$

iii) $$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$$

m, n are coprime odd

(Lagrange's Four-Square Thm)

(from book)