Lecture 24
March 9th, 2015

$s^2 \equiv -1 \bmod p$
$s^2 \equiv -1 \bmod q$

$p \equiv 1 \bmod 4$
$\{s^2 \equiv -1 \bmod p_1 \cdots p_r\}$ $2^r$

HW6.
#6(c). $S(n) = \#\{(x,y) : n = x^2+y^2, x \geq y > 0\}$

$\{(x,y) : n = x^2+y^2, x \geq 0, y \geq 0, \gcd(x,y)=1\} \leftarrow \{s^2 \equiv -1 \bmod n\}$
$(x,y) \rightarrow s \equiv \bar{x} y \bmod n$
$x\bar{x} \equiv 1 \bmod n$

Chapter 28 Primitive roots

Fermat's Little theorem $\Rightarrow a \not\equiv 0 \bmod p$ p prime
$a^{p-1} \equiv 1 \bmod p$
It is possible that some smaller power of a will be congruent to 1 mod p.

$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \cdots, p-1\}$ order $p-1$
order of element divide the order of a group

$(\mathbb{Z}/7\mathbb{Z})^\times$ $2^6 \equiv 1 \bmod 7$
$2^3 \equiv 1 \bmod 7$
$3^6 \equiv 1 \bmod 7$

$3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5$

6 is the smallest exponent

pattern: $p = 11$

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| $1^1 \equiv 1$ | $2^{10} \equiv 1$ | $3^5 \equiv 1$ | $4^5 \equiv 1$ | $5^5 \equiv 1$ | $6^{10} \equiv 1$ | $7^{10} \equiv 1$ | $8^{10} \equiv 1$ | $9^5 \equiv 1$ | $10^2 \equiv 1$ |

1. the smallest exponent $e$ so that $a^e \equiv 1 \bmod p$ divides $p-1$
2. There are always some $a$'s that require the exponent $p-1$

Def: $e_p(a)$ = the smallest exponent $e \geq 1$ s.t $a^e \equiv 1 \bmod p$
Exponent Divisibility Property: Suppose $\gcd(a,p)=1$, $a^n \equiv 1 \bmod p$
Then $e_p(a) \mid n$, In particular, $e_p(a) \mid p-1$

Look at number $a$ s.t. $e_p(a) \mid p-1$
Claim: $a, a^2, a^3, \cdots, a^{p-1} \bmod p$ are all distinct mod p
In other words, $\{a, a^2, \cdots, a^{p-1} \bmod p\} = \{1, 2, \cdots, p-1\}$
If $1 \leq i < j \leq p-1$, $a^i \equiv a^j \bmod p$, then $a^{j-i} \equiv 1 \bmod p$.
but $0 < j-1 < p-1$ . contradiction.

Def: A number $g$ with maximum possible exponent $e_p(g) = p-1$ is called a primitive root mod p.

e.g. For $p \equiv 11$, 2, 6, 7, 8 are primitive roots mod 11.
e.g. $3^6 \equiv 1 \bmod 7$, 6 is the smallest exponent.
$\phi(6) = 2$
$2^3 \equiv 1, 3^6 \equiv 1, 4^3 \equiv 1, 5^6 \equiv 1, 6^2 \equiv 1 \bmod 7$
3, 5 are primitive roots mod 7.

Thm (Primitive Root Thm) Every prime $p$ has a primitive root.

*More precisely, there are exactly $\phi(p-1)$ primitive roots mod $p$.*

(In terms of group theory, $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group).

Proof Idea: Take a certain set of numbers and count them in two different ways

"psi"

For each $d$ s.t. $d \mid p-1$, let $\psi(d)$ = the number of $a$'s with $1 \le a < p$ and $e_p(a) = d$

In particular, $\psi(p-1)$ = the number of primitive roots mod $p$

Claim: For any $d \mid p-1$, $\psi(d) = \phi(d)$

Proof: Step 1: Let $n \mid p-1$ and $_1, \cdots, d_r$ divisors of $n$.

prove next time. Then $\psi(d_1) + \cdots + \psi(d_r) = n$

Step 2: Since $\phi(d_1) + \cdots + \phi(d_r) = n$, $\phi(d_i) = \psi(d_i)$ $\forall i$

$\phi(1) = \psi(1) = 1$

If $n = q$ is a prime $\phi(q) + \phi(1) = q = \psi(q) + \psi(1)$

So $\phi(q) = \psi(q)$

Assume $\phi(d) = \psi(d)$ for any $d < n$, we prove

$\phi(n) = \psi(n)$

Let $d_1, \cdots, d_r$ be divisor of $n$

$d_2, \cdots, d_r < n$. By relabelling, we can assume $d_1 = n$

$\Rightarrow \phi(n) = \psi(n)$ $\qquad$ $\phi(n) + \underbrace{\phi(d_2) + \cdots + \phi(d_r)} = n = \psi(n) + \underbrace{\psi(d_2) + \cdots + \psi(d_r)}$

$d_2, \cdots d_r < n$

Artin's Primitive Root Conj.: there are inf many primes $p$ s.t. $2$ is a primitive root mod $p$.