Lecture 34, Nov. 11

34.1 Theorem (Fermat's Little Theorem)**.** *let p be a prime then*

1. *for all $a \in \mathbb{Z}$ such that $gcd(a, p) = 1$,*
$$a^{p-1} = 1 \mod p$$

2. *for all $a \in \mathbb{Z}$,*
$$a^p = a \mod p$$

34.2 Theorem (Euler-Fermat Theorem)**.** *Let $n \in \mathbb{Z}^+$. For all $a \in \mathbb{Z}$ with $gcd(a, n) = 1$,*

$$a^{\varphi(n)} = 1 \mod n$$

34.3 Example. Find 2^{-1} in $\mathbb{Z}_1 1$

Solution (Solution 1). In $\mathbb{Z}_1 1$, $2^{-1} = 6$ because $2 \cdot 6 = 12 = 1$.

Solution (Solution 2). Since $2^{10} = 1 \mod 11$ by Fermat's Little Theorem, so $2^{-1} = 2^9 = 6 \mod 11$.

34.4 Definition (Cyclic)**.** We say that a group G with $|G| = n$ is cyclic and is generated by $u \in G$ when

$$G =< u >= \{u^k \mid k \in \mathbb{Z}\}$$

Fact: When p is an odd prime, U_p^k is cyclic.

Remark.
$$U_1 1 =< 2 >=< 2^k > \text{ for all } k \in U_{10} =< 2 >=< 5 >=< 7 >=< 6 >$$

34.5 Example. Consider the Diophantine equation $x^2 + y^2 = n$ where $n \in \mathbb{N}$. Show that if $n = 3 \mod 4$ then there are no solutions.

Solution. In $\mathbb{Z}_4$,

x	0	1	2	3
x^2	0	1	0	1

For $x, y \in \mathbb{Z}_4$,

$$\begin{aligned} x^2 + y^2 \in& \{0 + 0, 0 + 1, 1 + 0, 1 + 1\} \\ =& \{0, 1, 2\} \end{aligned}$$

Solution. In $\mathbb{Z}_7$,

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
$3x^2$	0	3	5	6	6	5	3
$3x^2 + 4$	4	0	2	3	3	2	0

For $x, y \in \mathbb{Z}_7$, since $3x^2 + 4 = y^3$ in $\mathbb{Z}_7$,

It follows that if $3x^2 + 4 = y^3$ in $\mathbb{Z}_7$, then $x = 0, 6 \mod 7$ and $y = 0 \mod 7$.

34.6 Exercise. Try the example in $\mathbb{Z}_9$.

34.7 Example. Determine whether $2^{70} + 3^{70}$ is prime.

Solution. In $\mathbb{Z}_{13}$, powers repeat every 12, so $2^{70} + 3^{70} = 2^{10} + 3^{10} = 10 + 3 = 13$, thus $13 \mid 2^{70} + 3^{70}$

34.8 Theorem (Linear Congruence Theorem). *Let $n \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, let $d = gcd(a, n)$. Consider the equation*

$$ax = b \mod n$$

1. *The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$ if and only if $d \mid b$*
2. *If $x = u$ is a solution (so that $au = b \mod n$), then the general solution is*

$$x = u + k\frac{n}{d} \text{ for } k \in \mathbb{Z}.$$

Proof. This is essentially a restatement of the Linear Congruence Theorem (the LDET) because x is a solution to $ax = b$ mod $n \iff thereexistk \in \mathbb{Z} ax = b + kn \iff thereexisty \in \mathbb{Z} ax + ny = b$ ☐

Proof.

1. TFAE
   (a) The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$
   (b) Exists $x, y \in \mathbb{Z}$ such that $ax + ny = b$
   (c) $d \mid b$ (By LDET)
2. Suppose $x = u$ is a solution so that $au = b \mod n$. Thus by the LDET, the general solution to the equation $ax + ny = b$ is

$$(x, y) = u + k\frac{n}{d}, \ldots$$

Thus $u + k\frac{n}{d}$ are solutions.

☐