8/26/2026

Two important thms.

Thm (Euler) Let m be a positive integer and let $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Thm (Fermat) Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

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

Equivalently, $a^p \equiv a \pmod{p}$.

E.g. Simplify $2^{100} \pmod{13}$.

$p = 13$ is prime, $100 = 12 \cdot 8 + 4$.

Fermat $\Rightarrow 2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 3 \pmod{13}$.

Solving linear congruence equations

Thm. The linear equation $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, m)$, in which case there are exactly d solutions. Moreover, if x_0 is a solution, then every solution is of the form $x = x_0 + k \cdot \frac{m}{d}$, where k is any integer.

E.g. Solve $12x \equiv 18 \pmod{42}$.

$d = (12, 42) = 6$, $d \mid 18$. So it has 6 solutions.

Dividing by 6: $2x \equiv 3 \pmod{7}$ ($\frac{m}{d}$). $x_0 = 5$ is a solution.

So all the solutions are $x \equiv 5, 12, 19, 26, 33, 40 \pmod{42}$.

More generally, one may study polynomial congruences

$$f(x) \equiv 0 \pmod{m},$$

where $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with coefficients $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. (The set $\mathbb{Z}[x]$ of all polynomials with integer coefficients is a commutative ring under $+$ and $\times$, and in fact, a UFD)

Thm (Lagrange) Let p be a prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

with $p \nmid a_n$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n roots.

Pf. Exercise. Hint: Induction on n.

Note: Lagrange's thm may fail for a composite modulus:

$x^2 - 1 \equiv 0 \pmod 8$ has 4 roots: $x \equiv 1, 3, 5, 7 \pmod 8$.

Qudratic congruence equations.

A quadratic congruence equation in unknown x is of the form

$$ax^2 + bx + c \equiv 0 \pmod m,$$

where $a \not\equiv 0 \pmod m$.

Q: How to solve it? Think of

$$ax^2+bx+c=0.$$

Completing the square:

$$a\left(x^2+\frac{b}{a}x\right)+c=0$$

$$a\left(x^2+\frac{b}{a}x+\left(\frac{b}{2a}\right)^2-\left(\frac{b}{2a}\right)^2\right)+c=0$$

$$\left(x+\frac{b}{2a}\right)^2$$

$$a\left(x+\frac{b}{2a}\right)^2=\frac{b^2}{4a}-c=\frac{b^2-4ac}{4a}$$

Obervations: 1. Division is tricky and makes coefficients no longer integers.

2. Don't know if we can take $\sqrt{\ }$.

Reduction: Multiplying $ax^2+bx+c \equiv 0 \pmod m$ by $4a$:

$$4a^2x^2+4abx+4ac \equiv 0 \pmod{4am}.$$

$$\underbrace{4a^2x^2+4abx+b^2}_{(2ax+b)^2} - b^2 + 4ac \equiv 0 \pmod{4am}$$

$$(2ax+b)^2 \equiv \overbrace{b^2-4ac}^{\Delta} \pmod{4am}$$

Let $y = 2ax+b$. Then this is

$$y^2 \equiv \Delta \pmod{4am}.$$

Our task reduces to solving something like

$$x^2 \equiv a \pmod m.$$

Q: Solvable? If yes, how many solutions?

We will focus on $m=p$ is prime.

Lem. Let $p \geq 2$ be prime and $a \in \mathbb{Z}$ s.t. $p \nmid a$. Then

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

has no solution or 2 solutions.

Pf. Assume it has a solution x_0. Let x be any solution. Then

$$x_0^2 \equiv a \pmod{p} \qquad (1)$$

$$x^2 \equiv a \pmod{p}. \qquad (2)$$

$(2) - (1)$: $x^2 - x_0^2 \equiv 0 \pmod{p}$.

$$\Rightarrow (x + x_0)(x - x_0) \equiv 0 \pmod{p}.$$

So Euclid $\Rightarrow$ $x + x_0 \equiv 0 \pmod{p}$ or $x - x_0 \equiv 0 \pmod{p}$.

So $x \equiv -x_0 \pmod p$ or $x \equiv x_0 \pmod p$.

Note that $-x_0 \not\equiv x_0 \pmod p$.

Why: If $-x_0 \equiv x_0 \pmod p$, then $0 \equiv 2x_0 \pmod p$

Euclid $\Rightarrow p \mid 2$ or $p \mid x_0$, impossible because $p > 2$,

and $p \nmid a$ and $x_0^2 \equiv a \pmod p$. $\square$

Goal: Given a prime $p > 2$, determine all the values of

$a \in \mathbb{Z}$ $(p \nmid a)$ for which $x^2 \equiv a \pmod p$ is solvable.

Defn (Quadratic residues & nonresidues). An integer a, indivisible

by p, is a <u>quadratic residue</u> mod p if there is

$x \in \mathbb{Z}$ s.t. $x^2 \equiv a \pmod p$. Otherwise, a is called a

quadratic nonresidue mod p.

Notation: Write $a \; R \; p$ if a is a residue mod p,

$a \; N \; p$ if $-$ $-$ $-$ nonresidue mod p.

Eg. $1 \; R \; 3$: $x = 1$ solves $x^2 \equiv 1 \pmod 3$.

$-1 \; N \; 3$: $x^2 \equiv -1 \pmod 3$ is insolvable:

$1^2 \equiv 1 \pmod 3$, $2^2 \equiv 1 \pmod 3$.