$9 \mid 27$

$3 \mid 9$

$21 \mid 42$

$7 \mid 21$

Theorem:- If p is a prime number, and a and b are integers, then if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof:- $4 \mid (2 \cdot 2)$

$5 \mid 75$

Suppose $p \mid ab$ $5 \mid (15 \cdot 5)$

Case 1:- $p \mid a \Rightarrow$ Statement is true

Case 2:- $p \nmid a \Rightarrow ?$ $\gcd(a, p) = 1$

$\therefore \exists\ x, y \in \mathbb{Z}$ such that

$$ax + py = 1$$

$$axb + pyb = b$$

Since $p \mid ab$
$\Rightarrow ab = pn$
for some $n \in \mathbb{Z}$

$$xpn + pyb = b$$

$$p(xn + yb) = b$$

($xn + yb$: integer)

$\Rightarrow p \mid b$

The same proof applies if $p \nmid b$ to show that $p \mid a$.

Theorem:- For integers $a_1, a_2, \ldots, a_n$ and a prime number p.

If $p \mid a_1 a_2 a_3 \cdots a_n$

then $p \mid a_1$ or $p \mid a_2$ or $\cdots$ $p \mid a_n$

Fundamental Theorem of Arithmetic

Every integer $n \geq 2$, can be uniquely written in the form.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are prime numbers, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are non-negative integers.

$3 = 3$

$4 = 2 \cdot 2 = 2^2$

$12 = 2 \cdot 2 \cdot 3$
$= 2^2 \cdot 3$

$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$
$= 2^3 \cdot 3^2$

An integer n is a perfect square $n = x^2$ $x \in \mathbb{Z}$

16, 25

49, 43 not a perfect square.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = x^2 = \left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\right)^2$$
$$= p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k}.$$

$100 = 2^2 \cdot 5^2$

19(a) Show that 2^6+1 is not a prime

$a^2-b^2=(a-b)(a+b)$

a^3+b^3

$=(a+b)(a^2-ab+b^2)$

$a^4-b^4=(a^2-b^2)(a^2+b^2)$

a^4+b^4 cannot be factor.

a^6+b^6 .. .. ..

2^6+1

$(2^2)^3+1^3$

$(2^2+1)(2^4-2^2+1)$

$\therefore 2^2+1 \mid 2^6+1$

hence 2^6+1 is not a prime.

29 Let a, b be natural numbers with $\gcd(a,b)=1$ and ab a perfect square. Prove that a and b are also perfect squares.

A $ab=x^2$ for some $x\in\mathbb{Z}$

$ab=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} q_1^{\beta_1}q_2^{\beta_2}\cdots q_n^{\beta_n}$

$=x^2$

$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

$b=q_1^{\beta_1}q_2^{\beta_2}\cdots q_n^{\beta_n}$

Since $\gcd(a,b)=1$

hence p_i and q_i have no primes in common.

$\Rightarrow \alpha_1, \alpha_2, \cdots \alpha_k, \beta_1, \beta_2, \cdots \beta_n$ are multiples of 2.

This means a and b are perfect squares.

$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$

$\gcd(a,b)=p_1^{\min(\alpha_1,\beta_1)}p_2^{\min(\alpha_2,\beta_2)}\cdots p_k^{\min(\alpha_k,\beta_k)}$

$\operatorname{lcm}(a,b)=p_1^{\max(\alpha_1,\beta_1)}p_2^{\max(\alpha_2,\beta_2)}\cdots p_k^{\max(\alpha_k,\beta_k)}$

$20=2^2\cdot 5$

$21=3\cdot 7$

$20=2^2\cdot 3^0\cdot 5^1\cdot 7^0$

$21=2^0\cdot 3^1\cdot 5^0\cdot 7^1$

$20=2^2\cdot 5$

$16=2^4$

$\sim$ is transitive $\quad a, b \in \mathbb{Z} \setminus \{0\}$

$a \sim b$ if ab is a perfect square

$\iff ab = x^2 \quad x \in \mathbb{Z}$

Suppose $a \sim b$ and $b \sim c$

$\Rightarrow ab$ and bc are perfect squares.

$\Rightarrow ab = x^2$ and $bc = y^2$ for some $x, y \in \mathbb{Z}$

$\Rightarrow ab^2c = x^2 y^2$

$\Rightarrow ac = \frac{x^2 y^2}{b^2} = \left(\frac{xy}{b}\right)^2$

$\therefore a \sim c$.

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$.

$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$

$n = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} p_{k+1}^{\delta_{k+1}} \cdots$

$\gcd(a, n) = 1$ so there is no prime common between a and n.

This is also true for the pairs b and n and c and n.

$\therefore$ The prime decomposition of the product abc has no prime in common with n.

100 p q 10

O(n) pq RSA 2·5

4.4 Congruences

Let $n > 1$ be a natural number. and let $a, b \in \mathbb{Z}$. Then we say that a is congruent to b modulo n, iff $n \mid (a-b)$. In short, we write it as

$$a \equiv b \pmod{n}$$

$$18 \equiv 4 \pmod{7}$$

$$4 \equiv 18 \pmod{7}$$

$$13 \not\equiv 3 \pmod{4}$$

Properties of congruences $a, b, n \in \mathbb{Z}$, $n > 1$

1. $a \equiv a \pmod{n}$
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
3. If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for $c \in \mathbb{Z}$
4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a \pm c \equiv b \pm d \pmod{n}$ and $ac \equiv bd \pmod{n}$

   $(a-b) = nx$

   $ca = cb$

   $c(a-b) = cnx$

   $ca - cb = nx$ (1)
5. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for $k \in \mathbb{Z}^+$

   $a - b = nx$

   $(a-b)^k = (nx)^k = n^k x^k = n(\ldots)$

   $(a-b)^2 = a^2 - 2ab + b^2$

   $(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$

   $a^k - b^k$

   $(a-b)^{10}$
6. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$.

   If $d = \gcd(c, n) = 1$, then if $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n}$

   $8 \equiv 4 \pmod{2}$

   $2 \not\equiv 1 \pmod{2}$

   $2 \equiv 1 \pmod{1}$

Ex. $18 \equiv 4 \pmod 7$

Since $\gcd(2,7) = 1$

hence $9 \equiv 2 \pmod 7$

Congruence modulo n → Equivalence relation?

$a \sim b$ modulo n iff $a \equiv b \pmod n$

Reflexive ✓ $a \equiv a \pmod n$

Symmetric ✓ If $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

Transitive ✓ If $a \equiv b \pmod n$ and $b \equiv c \pmod n$

$\Rightarrow n \mid a-b$ $\quad b-c = ny$

$\Rightarrow a-b = nx$ $\quad x, y \in \mathbb{Z}$

$\Rightarrow (a-b)+(b-c) = nx+ny$

$a-c = n(x+y)$

$\Rightarrow n \mid (a-c)$

$\therefore a \equiv c \pmod n$

$\therefore$ Congruence modulo n is an equivalence relation

29 $a, b, c \in \mathbb{N}$ $\gcd(a,c) = 1$

and $b|c$ then $\gcd(a,b) = 1$

On the contrary suppose $\gcd(a,b) = d > 1$

$\Rightarrow d|a$ $d|b$

$\Rightarrow (d|a$ and $d|c)$ (as $d|b$ and $b|c$)

$ma + nb = 1$

$\not\Rightarrow \gcd(a,b) = 1$

$\gcd(12,9) = 3$

$3(12) + (-1)9 = 27$

$(1)12 + (-1)(9) = 3$

$-1575 = 7(-231) + 42$

$-231 = -6(42) + 21$

$42 = 2(21) + 0$

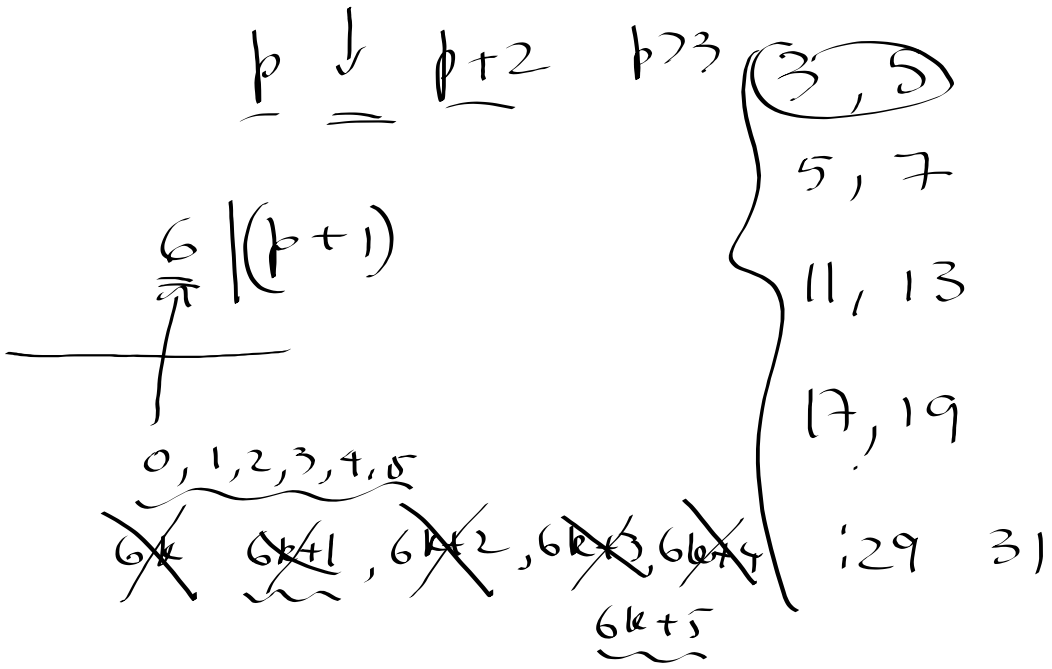
gcd

$\Rightarrow d$ is a common divisor of a and c

$\therefore \gcd(a,c) \geq d > 1$

$\Rightarrow \gcd(a,c) > 1$

Contradiction, hence $\gcd(a,b) = 1$.



Case 1 $p = 6k+1$

$p+2 = 6k+3 \leftarrow$ not a prime.

Case 2 $p = 6k+5$

$p+2 = 6k+7 = 6k_1+1$

$\Rightarrow p+1 = 6k+6 = 6(k+1)$

$6 \mid (p+1)$

2
3
5
7
11
13
17
19

$f(n) = n^2 + n + 11$

$f(1) = 1 + 1 + 11 = 13$

$f(2) = 17$ ✓

$f(11) = 11^2 + 11 + 11$

$= 11(\quad)$

Equivalence classes of the integers modulo n.

$a \in \mathbb{Z}$

$\bar{a} = \{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \}$

R equivalence rel.
A $a \in A$
$\bar{a} = \{ b \in A \mid aRb \}$

$n = 7$

$\bar{2} = \{ \ldots, -19, -12, -5, 2, 9, 16, 23, \ldots \}$

$\bar{0} = \{ \ldots, -21, -14, -7, 0, 7, 14, 21, \ldots \}$

$\bar{1} = \{ \ldots, -20, -13, -6, 1, 8, 15, 22, \ldots \}$

$\bar{3} = \{ \ldots, -18, -11, -4, 3, 10, 17, \ldots \}$

$\bar{4} = \{ \ldots, -17, -10, -3, 4, 11, 18, \ldots \}$

$\bar{5} = \{ \ldots, -16, -9, -2, 5, 12, 19, \ldots \}$

$\bar{6} = \{ \ldots, -15, -8, -1, 6, 13, 20, \ldots \}$

$\bar{8} = \{ \ldots, -13, -6, 1, 8, 15, 22, \ldots \}$

$\bar{1} = \bar{8}$

The congruence relation modulo n, partitions the set of integers $\mathbb{Z}$ into n equivalence classes, $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, (\overline{n-1})$.

For $0 \leq a \leq n-1$ $\quad a \in \mathbb{Z}$

$\bar{a} = \{ a + kn \text{ for some } k \in \mathbb{Z} \}$

$a \equiv b \pmod{n}$

$\Rightarrow n \mid (a - b)$

$\Rightarrow a - b = nk$

$b = a - n(k)$

$\Rightarrow a + n(-k)$

$4x = 16$

$x = 4$

Linear Congruence

$3x \equiv 4 \pmod 7$ — Solve this

$38x \equiv 41 \pmod 7$

$\downarrow$

$3x \equiv 6 \pmod 7$

$x \equiv 2 \pmod 7$

$x = 0$ $\quad 3 \cdot 0 \not\equiv 4 \pmod 7$

$x = 1$ $\quad 3 \cdot 1 \not\equiv 4 \pmod 7$

$x = 2$ $\quad 3 \cdot 2 \not\equiv 4 \pmod 7$

$x = 3$ $\quad 3 \cdot 3 \not\equiv 4 \pmod 7$

$x = 4$ $\quad 3 \cdot 4 \not\equiv 4 \pmod 7$

$x = 5$ $\quad 3 \cdot 5 \not\equiv 4 \pmod 7$

$x = 6$ $\quad 3 \cdot 6 \equiv 4 \pmod 7$ ✓

Solution: $x \equiv 6 \pmod 7$

Solving linear congruences

A linear congruence $ax \equiv b \pmod n$ has a solution iff $d \mid b$ where $d = \gcd(a, n)$.

If $d \mid b$, then it has d mutually incongruent solutions modulo n. If x_0 is one solution of the congruence, then the incongruent solutions are

$$x_0 + \frac{n}{d},\ x_0 + 2\left(\frac{n}{d}\right),\ x_0 + 3\left(\frac{n}{d}\right),\ \ldots,\ x_0 + (d-1)\left(\frac{n}{d}\right)$$

$2x \equiv 3 \pmod 4$ no solution

$\gcd(2, 4) \nmid 3$

$2x \equiv 4 \pmod 4$ has a solution

$65x \equiv 26 \pmod{169}$

$\gcd(65, 169) = 13$

$13 \mid 26$ hence the congruence has a solution

So the congruence has 13 incongruent solutions modulo 169.

$169 = 2(65) + 39$

$65 = 1(39) + 26$

$39 = 1(26) + 13$

$26 = 2(13) + 0$

$65x \equiv 26 \pmod{169}$

$65x - 26 = 169y$

$65x - 169y = 26$

$13 = 39 - 1(26)$

$= 39 - 1(65 - 39)$

$= 2(39) - 65$

$= 2(169 - 2(65)) - 65$

$13 = 2(169) - 5(65)$

$26 = 4(169) - 10(65)$

$26 = (-10)(65) - 169(-4)$

$\therefore x = -10 \equiv 159 \pmod{169}$

$(-10) \equiv 159 \pmod{169}$

$\therefore$ Solutions are

$$x \equiv 159 + \left(\frac{169}{13}\right)t \pmod{169}$$

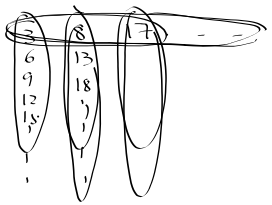
for $0 \le t \le 12$

$$x \equiv 159 + 13t \pmod{169} \quad 0 \le t \le 12$$

$t = 0 \quad x \equiv 159 \pmod{169}$

$t = 1 \quad x \equiv 172 \pmod{169} \Rightarrow x \equiv 3 \pmod{169}$

$t = 2 \quad x \equiv 185 \pmod{169} \Rightarrow x \equiv 16 \pmod{169}$



$x^2 - 3x + 2 = 0$

$x = 1, 2$

1, 2

11(d) $7x+2y \equiv 3 \pmod{15}$

$9x+4y \equiv 6 \pmod{15}$

x2

$14x+4y \equiv 6 \pmod{15}$

$5x \equiv 0 \pmod{15}$

$x \equiv 0 \pmod{3}$

$\Rightarrow$

$35x+10y \equiv 15 \pmod{15}$

$35x \equiv 0 \pmod{15}$

$10y \equiv 15 \pmod{15}$

$2y \equiv 3 \pmod{3}$

$2y \equiv 0 \pmod{3}$

$y \equiv 0 \pmod{3}$

$58x \equiv 6 \pmod{78}$

$78 = 1(58) + 20$

$58 = 2(20) + 18$

$20 = 1(18) + 2$ $\quad 2 \mid 6 \Rightarrow$ Solutions

$18 = 9(2) + 0$

$58x - 6 = 78y$

$58x - 78y = 6$

$2 = 20 - 18$

$= 20 - (58 - (2(20))$

$= 3(20) - 58$

$= 3(78 - 58) - 58$

$2 = 3(78) - 4(58)$

$6 = 9(78) - 12(58)$

$6 = (-12)(58) - (-9)(78)$

$-12 + \left(\frac{78}{2}\right)$

$x \equiv -12 + 39t \pmod{78}$

$0 \le t \le 1$