Whiteboard proofs and Examples

(1) if $a|b$ and $b|c$, then $a|c$

Proof:
$$a|b \Rightarrow \exists k_1 \in \mathbb{Z}: b = k_1 a$$
$$b|c \Rightarrow \exists k_2 \in \mathbb{Z}: c = k_2 b$$
$$c = k_2 \cdot k_1 a \qquad \text{Let } k = k_1 k_2$$
$$k \in \mathbb{Z}$$
$$c = k a$$
So $a|c$

(2) if $a|b$ and $a|c$, then $a|(mb+nc)$

Proof: $a|b \Rightarrow \exists d_1 \in \mathbb{Z}: b = d_1 a$

* $b = d_1 a \Rightarrow mb = m d_1 a$

Let $k_1 = m d_1$, $k_1 \in \mathbb{Z}$

So $mb = k_1 a$.

* $a|c \Rightarrow nc = k_2 a$

$$mb + nc = (k_1 + k_2) a$$
$$mb + nc = k a \qquad k = k_1 + k_2 \in \mathbb{Z}$$
Therefore $a|(mb+nc)$

(3) Proof that if $a \equiv b \pmod{m}$
$c \equiv d \pmod{m}$
then $a + c \equiv b + d \pmod{m}$.

Proof: $a \equiv b \pmod{m} \Rightarrow$

$a = k_1 m + r_1 \quad \ldots (1)$

$b = k_2 m + r_1 \quad \ldots (2)$

$c \equiv d \pmod{m} \Rightarrow$

$c = k_3 m + r_2 \quad \ldots (3)$

$d = k_4 m + r_2 \quad \ldots (4)$

$(1) + (3) \Rightarrow \quad a + c = (k_1 + k_3) m + (r_1 + r_2)$

$(2) + (4) \Rightarrow \quad b + d = (k_2 + k_4) m + (r_1 + r_2)$

$\Rightarrow a + c \equiv b + d \pmod{m}$

④ Theorem:

if $n \in \mathbb{N} > 1$ is composite $\Rightarrow \exists\, 1 < m \in \mathbb{N} \leq \sqrt{n}$: $m \mid n$.

Proof: n is composite $\Rightarrow$
$\exists\, a, b \in \mathbb{N} \neq 1, n$: $n = ab$.

Let $a \leq b$.

Assume $a > \sqrt{n}$ as $a < b$, then $b > \sqrt{n}$

So $a \times b > \sqrt{n} \times \sqrt{n} = n$

$a \times b > n$ contradiction with the initial statement $a \times b = n$.

Therefore it must be the case that $a \leq \sqrt{n}$.

$\square$

(5) Theorem: There are infinitely many Prims.

Proof:

Assume there are fintly many prime numbers i.e. the set S of prime numbers is finite.

Let $|S| = n$

$S = \{ P_1, P_2, P_3, \ldots, P_n \}$

Consider $P \in \mathbb{Z}$: $P = P_1 P_2 P_3 \cdots P_n + 1$

P is greater than all primes, so

$\Rightarrow$ p is not a prime

$\Rightarrow$ p is composite.

However: $\frac{P}{P_1}, \frac{P}{P_2}, \frac{P}{P_3}, \ldots, \frac{P}{P_n}$ will all have remainders $\Rightarrow$ no $P_i \in S$ are factors as they all have remainders.

$\Rightarrow$ so p is prime.

P is composite and p is prime $\Rightarrow$ Contradiction

Therefore, There are infinitely many Prims.

(6) Proof of Lemma

Let $a, b \in \mathbb{N}$ where $b \neq 0$ and let $a = bq + r$ where $0 \leq r < b$, then $\gcd(a,b) = \gcd(b,r)$

Proof:

Let d be a common divisor of a & b

Since $a = bq + r$, we have:

$$\underbrace{a}_{d|a} - \underbrace{bq}_{d|-bq} = r$$ so d is also a divisor of r

It follows that any divisor of a and b is also a divisor of b and r

Now: Let d be a common divisor of b and r

Since $a = bq + r$ we have that d divides a. Thus any divisor of b and r is a divisor of a and b.

It follows that the set of common divisors of a and b is the same as the set of common divisors of b and r. Thus $\gcd(a,b) = \gcd(b,r)$ $\square$

Example

Calculate gcd(19, 7) using Euclid's Algo.

$$19 = 7 \times 2 + 5$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + \underbrace{1^*}$$

$$2 = 1 \times 2 + 0$$

so the $\gcd(19,7) = \gcd(7,5) = \gcd(5,2)$

$= \gcd(2,1) = \gcd(1,0)$

The last nonzero remainder is 1, therefore $\gcd(19,7) = 1$

Bezout's theorem.

Let a and b natural mubers, then there are x and y : $\gcd(a,b) = xa + yb$

<u>Example</u>

$$\gcd(19,7) =$$

$$19 = 7\times 2 + 5 \Rightarrow 5 = 19 - 7\times 2$$

$$7 = 5\times 1 + 2 \Rightarrow 2 = 7 - 5\times 1$$

$$5 = 2\times 2 + 1 \Rightarrow 1 = 5 - 2\times 2$$

$$\begin{aligned}
1 &= 5 - 2\times 2 \\
&= 5 - 2(7 - 5\times 1) \\
&= 5 - 2\times 7 + 2\times 5 \\
&= 3\times 5 - 2\times 7 \\
&= 3(19 - 7\times 2) - 2\times 7 \\
&= 3\times 19 - 6\times 7 - 2\times 7
\end{aligned}$$

$$1 = \underbrace{3}_{\to x}\times 19 + \underbrace{(-8)}_{\to y}\times 7, \text{ so}$$

$$\gcd(19,7) = 1 = \underbrace{x\,19 + y\,7}_{\text{Diophantine equation}}$$

Solving congruence equations

e.g. $ax \equiv b \mod n$ has solutions iff
$\gcd(a, n) \mid b$.

if $\gcd(a, n) = c$, then the equation

$a x \equiv b \mod n$ will have c solutions

$\frac{n}{c}$ is how these solutions a far from each other.

e.g.$_1$ when $\gcd(n, a) = 1$

$2x \equiv 3 \mod 5$ $\gcd(2, 5) = 1$
one uniq solution

$3 \times 2x \equiv 3 \times 3 \mod 5$

$6x \equiv 9 \mod 5$

$x \equiv 4 \mod 5$ So the soluton to

our equation is $x = 4$.

Checking: $2x \equiv 3 \mod 5$

$2 \times 4/5 = 8/5$ We have $r = 3$

So $2 \times 4 \equiv 3 \mod 5$

$x = 4$ is the congruence class of the solution ie all members of this class are solutions to our eq $= \{4, 9, 14, 19, \dots\}$

e.g. 2 when $\gcd(a,n) > 1$

$$49x \equiv 28 \mod 119 \qquad \begin{cases} 49 = 7 \times 7 \\ 119 = 17 \times 7 \end{cases}$$

$$\gcd(49, 119) = 7$$

$$\frac{119}{7} = 17 \quad \ldots \text{(1)}$$

we try $x = 1, 2$ they are not solutions

$x = 3$ is a solution

Checking: $49 \times 3 = 147 = 119 \times 1 + \underline{28}$ ✓

$x_1 = 3$ is a solution

from (1) we know that $x + 17$ is also a solution and that there are 7 solutions

$x_2 = 20 \qquad x_4 = 54 \qquad x_6 = 88$

$x_3 = 37 \qquad x_5 = 71 \qquad x_7 = 105$

each solution is infinite (congruence class)

e.g. $X_1 = \{3, 122, 241, 360, \ldots\}$

$X_2 = \{20, 139, \ldots\}$

$X_3 = \{37, 156, \ldots\}$

$\vdots$

eg 3:

$$17x \equiv 3 \mod 29 \quad \ldots\ldots (1)$$

if one can find a number $v \in \mathbb{N}$, such that $17v \equiv 1 \mod 29$, then multiplying both sides of eq. (1) by v will give

$$v.17.x \equiv v.3 \mod 29 \quad \ldots\ldots (2)$$

def: v is called a multiplicative inverse of x in mod 29.

from (2) we get $X \equiv 3v \mod 29$ as $17v \equiv 1 \mod 29$

So as soon as we find v we can get x.

Compute v: using Euclid's algorithm as follows:

$$17v \equiv 1 \mod 29 \Rightarrow 17v = 1 - 29w$$

$$\Rightarrow 17v + 29w = 1$$

$29 = 1 \times 17 + 12$
$17 = 1 \times 12 + 5$
$12 = 2 \times 5 + 2$
$5 = 2 \times 2 + 1$

$12 = 29 - 17$
$\Rightarrow 5 = 17 - 12$
$2 = 12 - 2 \times 5$
$1 = 5 - 2 \times 2$

$1 = 5 - 2 \times 2$
$= 5 - 2 \times (12 - 2 \times 5)$
$= 5 \times 5 - 2 \times 12$
$= 5 \times (17 - 12) - 2 \times 12$
...

...
$1 = 12 \times 17 - 7 \times 29$
$1 = 17 \times 12 + 29 \times (-7)$
$\Rightarrow 17 \times 12 \equiv 1 \mod 29$

$\boxed{v = 12}$

eq. (2) $v.17.X = v.3 \mod 29$
$X \equiv v.3 \mod 29$
$X \equiv 36 \mod 29$
$X \equiv 7 \mod 29$

$X = \{7, 36, 65, \ldots\}$