An application

Theorem (Fund. Thm. of Arithmetic)

Every $n \in \mathbb{N}$ can be written uniquely (up to the order of the factors) as a product of primes

Pf: Two parts

(i) existence: every n can be written as a product of primes ✓ (we proved by strong induction)

(ii) uniqueness: HW.

Ex's ① $21 = 3 \cdot 7 = 7 \cdot 3$

no other way to factor into primes!

$21 \neq$ ~~[illegible]~~ $\neq 5 \cdot 5$

$\neq 2 \cdot 2 \cdot 5$

$\neq 2 \cdot 11$

② $200 = 2 \cdot 100$

$= 2 \cdot 2 \cdot 50$

$= 2 \cdot 2 \cdot 2 \cdot 25$

$= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$

$= 2^3 \cdot 5^2$

③ $97 = 97$ (is prime)

(ii)

13

We proved the following theorem day 1, but let's prove again (uses FTCA)

Theorem: There are infinitely many primes.

Pf: - Sps there are only finitely many primes $p_1, \dots, p_N$

- Define $P = p_1 \cdot p_2 \cdots p_N + 1$
- By FTCA P has a prime factorization, in particular P is divisible by some prime p.
- must have $p = p_j$ for some j $1 \le j \le N$.
- so $P = p_j \cdot K$

OTOH: $P = p_j \underbrace{(p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_N)}_{M} + 1$
$= p_j M + 1$

- so: $P = p_j \cdot K = p_j \cdot M + 1$

$\Rightarrow p_j K - p_j M = 1$
$\Rightarrow p_j (K - M) = 1$
$\Rightarrow p_j \mid 1$, a contradiction

ex: - proof actually shows that if $\{p_1, \dots, p_N\}$ is any set of primes then $P = p_1 \cdots p_N + 1$ is divisible by some $p \notin \{p_1, \dots, p_N\}$

- e.g. consider $\{3, 5, 7\}$

$3 \cdot 5 \cdot 7 + 1 = 105 + 1 = 106$
$= 2 \cdot 53$ ← not 3, 5, or 7

(iii)

Modular arithmetic

Recall: if $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ then $a \equiv b \pmod n$ means $n \mid b-a$.

- $\equiv \pmod n$ is equiv. relation
- $\mathbb{Z}/n\mathbb{Z}$ denotes set of equiv. classes.

$$\mathbb{Z}/n\mathbb{Z} = \{ [a]_n \mid a \in \mathbb{Z} \}$$

We took next result for granted, let's prove it now:

Prop'n Fix $n \in \mathbb{N}$, and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod n$ iff a, b have the same remainder when divided by n.

Pf: By the division algorithm, $\exists$ unique integers q_1, r_1, q_2, r_2 with $0 \leq r_1 < n$ $0 \leq r_2 < n$ s.t.

$$a = q_1 n + r_1$$
$$b = q_2 n + r_2$$

So: $$b - a = q_2 n + r_2 - (q_1 n + r_1)$$
$$= (q_2 - q_1) n + (r_2 - r_1)$$

($\Rightarrow$) - assume $a \equiv b \pmod n$

- then $n \mid b-a$, i.e. $b - a = kn$ for some $k \in \mathbb{Z}$
- hence $kn = (q_2 - q_1) n + (r_2 - r_1)$

(iv)

$\Rightarrow (k-(q_2-q_1))n = r_2 - r_1$
$\Rightarrow n \mid r_2 - r_1$

but $0 \le r_2, r_1 < n$

$0 \le r_2 < n$
$0 \le r_1 < n$

so $-n < r_2 - r_1 < n$
i.e. $|r_2 - r_1| < n$

$-r_1 > -n$
$\Rightarrow -n < r_2 - r_1 < n$

but then $n \mid r_2 - r_1 \Rightarrow r_2 - r_1 = 0$ ✓
$r_2 = r_1$ ✓

($\Leftarrow$) Sps $r_2 = r_1$
- then $b - a = (q_2 - q_1)n$
$\Rightarrow n \mid b - a$
$\Rightarrow a \equiv b \pmod{n}$ ✓

ex: $17 \equiv 37 \pmod 4$
- could check directly: $4 \mid 37-17$
- or could observe
$17 = 4 \cdot 4 + 1$
$37 = 4 \cdot 9 + 1$ } same remainder
- so that
$17 \equiv 37 \equiv 1 \pmod 4$

Since only possible remainders when dividing by n are $0, 1, \ldots, n-1$ this justifies another fact:

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

consists of exactly n distinct equiv. classes.

(v)

on HW you guys proved:
(modular arithmetic lemma)

Prop'n Fix $n \in \mathbb{N}$, $a, b, k, k' \in \mathbb{Z}$

① if $a \equiv b \pmod{n}$, $k \equiv k' \pmod{n}$
then $a + k \equiv b + k' \pmod{n}$

② if $a \equiv b \pmod{n}$, $k \equiv k' \pmod{n}$
then $ak \equiv bk' \pmod{n}$

Examples

① $6 \equiv 21 \pmod{5}$
and $12 \equiv 2 \pmod{5}$
Prop'n says: $6 + 12 \equiv 21 + 2 \pmod{5}$
indeed if we check:
$18 \equiv 23 \equiv 3 \pmod{5}$
Prop'n also says: $6 \cdot 12 \equiv 21 \cdot 2 \pmod{5}$
Indeed: $72 \equiv 42 \equiv 2 \pmod{5}$

② Prop'n says can manipulate congruency w/ $\equiv$ like equation w/ $=$ with respect to $+$ and $\cdot$
e.g. if $x, y \in \mathbb{Z}$ and
$x \equiv y \pmod{7}$
then $x + 3 \equiv y + 3 \pmod{7}$ "add 3 to both sides"
and $3x \equiv 3y \pmod{7}$ "mult. 3 to both sides"

or even better, since $3 \equiv 10 \pmod{7}$
can conclude:
$x + 3 \equiv y + 10 \pmod{7}$
$3x \equiv 10y \pmod{7}$

(vi)

subtraction works too, since subtracting c is just adding $-c$.

e.g. if I know
$$a \equiv b \pmod{11}$$
then $a-3 \equiv b-3 \pmod{11}$ "subtract 3 from both sides"

but since $-3 \equiv 8 \pmod{11}$ could have also written
$$a-3 \equiv b+8 \pmod{11}.$$

③ Can use these kinds of manipulations to "solve congruences"

e.g. find all $x \in \mathbb{Z}$ s.t.

$$\begin{array}{ccc} 652x & \equiv & x+23 \pmod 5 \\ \text{III} & & \text{III} \\ 2x & \equiv & x+2 \pmod 5 \end{array}$$

(subtract x) $\Rightarrow x \equiv 2 \pmod 5$ ✓

So set of solutions is $x \in [2]_5$
$= \{ \ldots, -3, 2, 7, 12, \ldots \}$

On the other hand division on both sides is not allowed in general.

ex: ① - Fix $x \in \mathbb{Z}$
- Sps $2x \equiv 1 \pmod 3$
- writing "$x \equiv 1/2 \pmod 3$" is meaningless

② Observe: $15 \equiv 21 \pmod 6$
- if we "divide both sides by 3" we get:
$$5 \equiv 7 \pmod 6$$
which is false.

③ Observe: $8 \equiv 22 \pmod 7$
- if we divide both sides by 2 we get:
$$4 \equiv 11 \pmod 7$$
which is true.

↳ So what gives?
The reason: 2 has a multiplicative inverse in $\mathbb{Z}/7\mathbb{Z}$, while 3 does not have such an inverse in $\mathbb{Z}/6\mathbb{Z}$.
↳ more on this later.

Positive exponentiation is always ~~[illegible]~~ allowed over $\equiv$

<u>Prop'n</u> Fix $a, b \in \mathbb{Z}$ and $k, n \in \mathbb{N}$.
if $a \equiv b \pmod{n}$
then $a^k \equiv b^k \pmod{n}$

<u>Pf</u>: Follows immediately from modular arithmetic lemma and induction:

$$\text{if } a \equiv b \pmod{n}$$
$$\text{then } a^2 \equiv b^2 \pmod{n}$$
$$\vdots$$
$$a^k \equiv b^k \pmod{n}$$

<u>Ex</u>: ① Since $7 \equiv 2 \pmod{5}$

we have $7^3 \equiv 2^3 \pmod{5}$
$\equiv 8 \pmod{5}$
$\equiv 3 \pmod{5}$.

get this w/o actually computing 7^3.

② Find the last digit of $2033 \cdot 719 + 27$. ~~[illegible]~~

20

Sol'n: last digit is exactly remainder when divided by 10.

Observe:

$$2033 \cdot 719 + 27 \equiv 3 \cdot 9 + 7 \pmod{10}$$
$$\equiv 27 + 7 \pmod{10}$$
$$\equiv 34 \pmod{10}$$
$$\equiv 4 \pmod{10}$$

$\Rightarrow$ last digit is 4

and indeed:

$$2033 \cdot 719 + 27 = 1,461,754 \checkmark$$

3 Find the remainder of 2^{37} when divided by 47.

Sol'n: $2, 4, 8, 16, 32, \underset{\overset{\shortparallel}{2^6}}{64} = 47 + 17$

$$2^6 \equiv 64 \equiv 17 \pmod{47}$$

$$\Rightarrow (2^{12}) = (2^6)^2 \equiv \underset{\substack{\shortparallel \\ 289 \\ \shortparallel \\ 47 \cdot 6 + 7}}{17^2} \pmod{47}$$

$$\equiv 7 \pmod{47}$$

$$\Rightarrow 2^{24} = (2^{12})^2 \equiv 7^2 \pmod{47}$$
$$\equiv 49 \pmod{47}$$
$$\equiv 2 \pmod{47}$$

new:

$$2^{37} = 2^{24} \cdot 2^{12} \cdot 2$$
$$\equiv 2 \cdot 7 \cdot 2 \pmod{47}$$
$$\equiv 28 \pmod{47}$$

So 28 is remainder of 2^{37} when divided by 47 ✓

Multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$

Def'n Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then we say a has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ iff $\exists b \in \mathbb{Z}$ s.t.

$$ab \equiv 1 \pmod{n}$$

We sometimes write $b = a^{-1}$ not unique but unique up to $\equiv$ class

ex: 3 has a mult. inv. in $\mathbb{Z}/7\mathbb{Z}$ since $3 \cdot 5 = 15 \equiv 1 \pmod 7$

Prop'n: Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then a has a mult. inv. in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a, n) = 1$.

Pf: ($\Rightarrow$) assume first $\exists b \in \mathbb{Z}$ s.t.
$ab \equiv 1 \pmod{n}$

- then $n \mid 1-ab$
- i.e. $\exists k \in \mathbb{Z}$

$kn = 1-ab$

so: $ab + kn = 1$ i.e. $ab + nk = 1$

~~$b(a) + k(n) = 1$~~ ~~$ab + nk = 1$~~

i.e. 1 is a linear combo of a, n

$\Rightarrow$ by Bezout $\gcd(a,n) = 1$ ✓

($\Leftarrow$) - Now assume $\gcd(a,n) = 1$

Bezout: - then $\exists\, b, k \in \mathbb{Z}$ s.t.

$ab + nk = 1$

so $nk = 1-ab$

so $n \mid 1-ab$

so $ab \equiv 1 \pmod{n}$ ✓

Ex's: ① $5x \equiv 1 \pmod{21}$ does have a solution, since $\gcd(5,21) = 1$

indeed $x = 17$ works since

$5 \cdot 17 = 85 = \underset{21\cdot 4}{84} + 1 \equiv 1 \pmod{21}$

note: -17 is not unique solution, but is unique up to equiv. class

- e.g. $-4 \equiv 17 \pmod{21}$
  and $5 \cdot (-4) = -20 = -21 \cdot 1 + 1$
  $\equiv 1 \pmod{21}$

- set of solutions to
  $5x \equiv 1 \pmod{21}$
  is exactly $[17]_{21}$

- might write
  $[5]_{21} \cdot [17]_{21}$ "=" $[1]_{21}$
  i.e. $\forall a \in [5]_{21}$
  $\forall b \in [17]_{21}$
  $ab \in [1]_{21}$ i.e. $ab \equiv 1 \pmod{21}$

(2) - The congruence $6x \equiv 1 \pmod{21}$ has no sol'n

- such an x would be a mult. inv. of 6 in $\mathbb{Z}/21\mathbb{Z}$.
- but $\gcd(6, 21) = 3 \neq 1$ so no such x exists.

(3) Find all solutions $x \in \mathbb{Z}$ to:
$4x \equiv 5 \pmod{7}$

Sol'n Since 7 is prime and $7 \nmid 4$

we must have
$$\gcd(4,7)=1$$
so 4 has a mult. inverse in
$\mathbb{Z}/7\mathbb{Z}$

and indeed:
$$4\cdot 2 = 8 \equiv 1 \pmod 7$$
so $2 = 4^{-1}$

↳ instead of "dividing both sides of $4x \equiv 5$ by 4"
can multiply both sides by 2:

$$4x \equiv 5 \pmod 7$$
$$\Leftrightarrow \quad 2\cdot 4x \equiv 2\cdot 5 \pmod 7$$
$$\Leftrightarrow \quad 8x \equiv 10 \pmod 7$$
$$\Leftrightarrow \quad x \equiv 10 \pmod 7$$
$$\Leftrightarrow \quad x \equiv 3 \pmod 7$$

and if $x \equiv 3 \pmod 7$
then $4x \equiv 12 \equiv 5 \pmod 7$
so $4x \equiv 5 \Leftrightarrow x \equiv 3 \pmod 7$
i.e.
$[3]_7$ is set of sol'ns ✓

(i)

25

<u>Prop'n</u> For any $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ there is a sol'n to $ax \equiv b \pmod{n}$ iff $\gcd(a,n) \mid b$.

<u>Pf</u>: Let $d = \gcd(a,n)$

($\Rightarrow$) Assume there is a sol'n to $ax \equiv b \pmod{n}$, i.e. $\exists\, l \in \mathbb{Z}$ $al \equiv b \pmod{n}$

i.e. $n \mid b - al$

so $\exists k$ s.t. $nk = b - al$

$\Rightarrow al + nk = b$

So since $d \mid a$ and $d \mid n$

i.e. $dp = a$ and $dq = n$

we have

$dpl + dqn = b$

$\Rightarrow d(pl + qn) = b$

$\Rightarrow d \mid b$ ✓

($\Leftarrow$) Now assume $d \mid b$

i.e. $\exists l$ $dl = b$

By Bezout $\exists\, k, k' \in \mathbb{Z}$

$ak + nk' = d$

$\Rightarrow akl + nk'l = dl = b$

$\Rightarrow nk'l = b - a(kl)$

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

$\Rightarrow a(kl) \equiv b \pmod{n}$ $\Rightarrow x = kl$ is a sol'n ✓

(ii)

Ex's ① There is a sol'n to $6x \equiv 4 \pmod 8$

why: $\gcd(6,8) = 2$ and $2 \mid 4$ ✓
indeed: $x = 2$ works ✓

② There is no sol'n to
$4x \equiv 3 \pmod 8$
why: $\gcd(4,8) = 4$
and $4 \nmid 3$ ✓

Euclidean Algorithm

↳ lots of our results depend on knowing some gcd.
↳ How do we compute $\gcd(a,b)$ for (potentially large) $a, b \in \mathbb{Z}$?
Euclidean Algorithm!

Lemma: Fix $a, b, q, r \in \mathbb{Z}$
If $a = bq + r$
then $\gcd(a,b) = \gcd(b,r)$

Pf: Let $d = \gcd(a,b)$
$d' = \gcd(b,r)$

(iii)

<u>Observe</u>: - since $a = bq + r$ and $d' | b$ and $d' | r$ we know $d' | a$

- so $d' \leq d$ ← gcd(a,b)

<u>CTOH</u>: - By Bezout $\exists m, n \in \mathbb{Z}$ s.t.

$rm + bn = d'$

- but $r = a - bq$ so:

$(a-bq)m + bn = d'$

i.e. $am + b(n - qm) = d'$

- so d' is a linear combo of a, b

$\Rightarrow d' \geq d$

so $d' = d$ ✓

↪ Lemma allows us to find gcd(a,b) by repeatedly "reducing by remainders"

<u>Thm</u> (Euclidean Algorithm)

Fix $a, b \in \mathbb{N}$ with $a \geq b$

Define a finite decreasing sequence by

$r_0 = a \qquad r_1 = b$

$r_j = r_{j+1} q_{j+1} + r_{j+2}$

where $0 \leq r_{j+2} < r_{j+1}$

(iv)

If $r_n = 0$ we define r_n as the last term.

Then: $r_{n-1} = \gcd(a,b)$

$\hookrightarrow$ proof follows from Lemma but let's skip + see examples.

Ex ① Find $\gcd(68,12)$

Sol'n $a = 68 = r_0$ $\quad b = 12 = r_1$

$$\underset{r_0}{68} = \underset{r_1}{12} \cdot \underset{q_1}{5} + \underset{r_2}{8}$$
$$\underset{r_1}{12} = \underset{r_2}{8} \cdot 1 + \underset{r_3}{4}$$
$$\underset{r_2}{8} = \underset{r_3}{4} \cdot 2 + \underset{r_4}{0}$$

so $r_4 = 0 \Rightarrow r_3 = 4$ is $\gcd(68,12)$!

Why: By Lemma:

$$\gcd(68,12) = \gcd(12,8) = \gcd(8,4) = 4 \checkmark$$

(v)

(2) Find $m, n \in \mathbb{Z}$ s.t.

$$68m + 12n = 4$$

Sol'n: Bezout says: m, n exist
Euclid gives us way to find m, n!

$$\begin{aligned} 4 &= 12 - 8 \cdot 1 \\ &= 12 - (68 - 12 \cdot 5) \cdot 1 \\ &= 12 - 68 \cdot 1 + 12 \cdot 5 \\ &= 12 \cdot 6 + 68(-1) \end{aligned}$$

so $m = -1$ $n = 6$ works!

↳ this method of back substitution to find m, n is sometimes called the extended EA.

(3) Find $k, l \in \mathbb{Z}$ s.t.

$$64k + 111l = 1$$

Sol'n: For this to be possible must be that $\gcd(64, 111) = 1$

3C

(vi)

Let's do EA:

$$111 = 64 \cdot 1 + 47$$
$$- \quad 64 = 47 \cdot 1 + 17$$
$$- \quad 47 = 17 \cdot 2 + 13$$
$$- \quad 17 = 13 \cdot 1 + 4$$
$$* \quad 13 = 4 \cdot 3 + 1 \leftarrow \gcd(64, 111) \checkmark$$
$$4 = 4 \cdot 1 + 0$$

now we go backwards from $*$:

$$1 = 13 - 4 \cdot 3 \qquad \text{but: } 4 = 17 - 13 \cdot 1$$
$$1 = 13 - (17 - 13 \cdot 1) \cdot 3$$
$$= 13 - 17 \cdot 3 + 13 \cdot 3$$
$$= 13 \cdot 4 - 17 \cdot 3$$
$$= 17(-3) + 13(4) \qquad \text{but: } 13 = 47 - 17 \cdot 2$$
$$= 17(-3) + (47 - 17 \cdot 2)(4)$$
$$= 47(4) + 17(-3) + 17(-8)$$
$$= 47(4) + 17(-11) \qquad \text{but } 17 = 64 \cdot 1 - 47$$
$$= 47(4) + (64 \cdot 1 - 47)(-11)$$
$$= 64(-11) + 47(4) + 47(11)$$
$$= 64(-11) + 47(15) \qquad \text{but } 47 = 111 - 64 \cdot 1$$
$$= 64(-11) + (111 - 64 \cdot 1)(15)$$
$$= 111(15) + 64(-11) + 64(-15)$$
$$= 111(15) + 64(-26)$$

so $k = -26$ and $\ell = 15$ work $\checkmark$