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 $n \in \mathbb{N}$ can be written as a product of primes. (√)

(ii) **Uniqueness:** HW.

**Ex's**

1. $21 = 3 \cdot 7 = 7 \cdot 3$
   
   No other way to factor into primes!

   $21 \neq 5 \cdot 5$
   
   $\neq 2 \cdot 2 \cdot 5$
   
   $\neq 2 \cdot 11$

2. $200 = 2 \cdot 100$
   
   $= 2 \cdot 2 \cdot 50$
   
   $= 2 \cdot 2 \cdot 2 \cdot 25$
   
   $= 2 \cdot 2 \cdot 5 \cdot 5$
   
   $= 2^3 \cdot 5^2$

3. $97 = 97$ (is prime)
We proved the following theorem on day 1, but let's prove again (use FTOA).

**Theorem:** There are infinitely many primes.

**PF:** Suppose there are only finitely many primes: $p_1, \ldots, p_N$.

- Define $P = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$.
- By FTOA, $P$ has a prime factorization, in particular $P$ is divisible by some prime $p_j$ for some $j$ such that $1 \leq j \leq N$.
- So $P = p_j \cdot k$.

OTOH: $P = p_j \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_N + 1) = p_j \cdot M + 1$.

So $P = p_j \cdot k = p_j \cdot M + 1$.

Thus, $p_j \cdot k = p_j \cdot M + 1$ implies $p_j \cdot (k - M) = 1$.

By definition of $k$, $k - M < 0$, a contradiction.

Example: Recall actually shows that if $\mathfrak{c}$ is any set of primes, then $P = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$ is divisible by some $p \not\in \{p_1, \ldots, p_N\}$.

E.g. Consider $\{3, 5, 7\}$.

$3 \cdot 5 \cdot 7 + 1 = 106 + 1 = 107$, prime.
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.
\[
\begin{align*}
a &= q_1 n + r_1 \\
b &= q_2 n + r_2
\end{align*}
\]

So:
\[
\begin{align*}
b - a &= q_2 n + r_2 - (q_1 n + r_1) \\
&= (q_2 - q_1) n + (r_2 - r_1)
\end{align*}
\]

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

but \( 0 \leq r_2, r_1 < n \)
\( 0 \leq r_2 < n \)
\( 0 \leq r_1 < n \)

so \( -n < r_2-r_1 < n \)
\( \Rightarrow -r_2+r_1 < n \)
\( \Rightarrow 1r_2-r_1 < n \)
\( \Rightarrow n \mid r_2-r_1 = r_2 = r_1 \)

(\( \Leftarrow \)) \( \text{Suppose } r_2 = r_1 \)
\( \Rightarrow n \mid b-a = (q_2-q_1)n \)
\( \Rightarrow n \mid b-a \)
\( \Rightarrow a \equiv b \pmod{n} \)

\( \text{Ex.2} \) \( 17 \equiv 37 \pmod{4} \)
\( \rightarrow \) could check directly: \( 4 \mid 37-17 \)
\( \rightarrow \) or could observe
\( 17 = 4 \cdot 4 + 1 \)
\( 37 = 4 \cdot 9 + 1 \) \( \rightarrow \) same remainder

\( \rightarrow \) so that
\( 17 \equiv 37 \equiv 1 \pmod{4} \)

Since only possible remainders when dividing by \( n \) are \( 0, 1, ..., n-1 \)
this justifies another fact:

\( \mathbb{Z}/n\mathbb{Z} = \{ [0], [1], ..., [n-1] \} \)

consists of exactly \( n \) distinct
equiv. classes.
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 $a k \equiv b k' \pmod{n}$

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
   $= \equiv$ 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
\[ a - 3 \equiv b - 3 \pmod{11} \]

But since \(-3 \equiv 8 \pmod{11}\)

Could have also written
\[ a - 3 = b + 8 \pmod{11} \]

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

E.g. And all \(x \in \mathbb{Z}\) s.t.

\[ 652x \equiv x + 23 \pmod{5} \]
\[ 111 \]
\[ 2x \equiv x + 2 \pmod{5} \]

(subtract \(x\)) \(\Rightarrow x \equiv 2 \pmod{5} \)

So set of solutions is \(\{ \ldots, -3, 2, 7, 12, \ldots \} \)

On the other hand, division is not allowed in general.
ex: 1. Fix $x \in \mathbb{Z}$
   - Show: $2x \equiv 1 \pmod{3}$
   - Writing "$x \equiv \frac{1}{2} \pmod{3}$" is meaning "$x$ is inverse of 2 in $\mathbb{Z}/3\mathbb{Z}$".

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 5 does not have such an inverse in $\mathbb{Z}/6\mathbb{Z}$.
  - More or less later.
Positive exponents are always allowed over $\equiv$.

Prop: Fix $a, b \in \mathbb{Z}$ and $k, n \in \mathbb{N}$.

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

Then $a^k \equiv b^k \pmod{n}$

Proof: Follow immediately from modular arithmetic lemma and induction:

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

Then $a^2 \equiv b^2 \pmod{n}$

$\therefore c^k \equiv b^k \pmod{n}$

Ex. 0 Since $7 \equiv 2 \pmod{5}$

We have $7^3 \equiv 2^3 \pmod{5}$

$\equiv 8 \pmod{5}$

$\equiv 3 \pmod{5}$

Find the last digit of $1^k$?

7873. $719 + 27$. 0000
Solution: Last digit is exactly remainder when divided by 10.

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

⇒ Last digit is 4

and indeed:

\[
2033 \cdot 719 + 27 = 1,461,754.
\] 

3. Find the remainder of \(2^{57}\) when divided by 47.

Solution: 2, 4, 8, 16, 32, 64 = 47 + 17

\[
2^6 = 64 \equiv 17 \pmod{47} \\
= 3 \cdot (2^{12}) = (2^6)^2 \equiv 17^2 \pmod{47}
\]

\[
2^{54} = (2^{12})^9 \equiv 7 \pmod{47} \\
\Rightarrow 2^{29} = (2^{12})^2 \equiv 7^2 \pmod{47} \\
\equiv 49 \pmod{47} \\
\equiv 2 \pmod{47}
\]
New:
\[ 2^{34} = 2^{24} \cdot 2^{12} \cdot 2 \equiv 2 \cdot 7 \cdot 2 \pmod{47} \]
\[ \equiv 28 \pmod{47} \]

So, 28 is the remainder of 2^{34} when divided by 47.

**Multiplicative inverses in \( \mathbb{Z}/n\mathbb{Z} \)**

**Definition:** Fix \( n \in \mathbb{N} \) and \( a \in \mathbb{Z} \). Then we say \( a \) has a multiplicative inverse in \( \mathbb{Z}/n\mathbb{Z} \) if \( \exists b \in \mathbb{Z} \) s.t. \( ab \equiv 1 \pmod{n} \).

We sometimes write \( b = a^{-1} \%

**Example:** 3 has a mult. inv. in \( \mathbb{Z}/7\mathbb{Z} \)

Since \( 3 \cdot 5 = 15 \equiv 1 \pmod{7} \)

**Proof:** Fix \( n \in \mathbb{N} \) and \( a \in \mathbb{Z} \). Then \( a \) has a mult. inv. in \( \mathbb{Z}/n\mathbb{Z} \) if \( \gcd(a, n) = 1 \).
\textbf{Proof:} (\(\Rightarrow\)) Assume first \(fb \in \mathbb{Z}\) s.t.
\[ab \equiv 1 \pmod{n}\]
- then \(n|1-ab\)
- \(-1 = \exists k \in \mathbb{Z}\)
\[kn = 1-ab\]
so:
\[ab + kn = 1\]
\[
\therefore\quad\text{l.c. } ab + nk = 1\]
\[
\therefore\quad 1 \text{ is a linear combo of } ab\]
\[
\Rightarrow \text{ by Bezout } \gcd(ab, n) = 1\]

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

\textbf{Bezout:} - then \(\exists b, k \in \mathbb{Z}\) s.t.
\[ab + nk = 1\]
so
\[nk = -(ab)\]
so
\[n|1-ab\]
so
\[ab \equiv 1 \pmod{n}\]

\textbf{Ex's:}\n\[5 \times 2 \equiv 1 \pmod{21}\] does
\textbf{not} have a solution, since
\[\gcd(5, 21) = 1\]
Indeed \(x = 17\) works since
\[5 \times 17 = 85 = 84 + 1 \equiv 1 \pmod{21}\]
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
  \(5x \equiv 1 \pmod{21}\)

- exactly \([17]_{21}\)
  - might think
  \([5]_{21} \cdot [17]_{21} = [1]_{21}\)
  i.e. \(5a \equiv [5]_{21}\)
  \(4b \equiv [17]_{21}\)
  \(ab \equiv [1]_{21}\) (i.e. \(ab \equiv 1 \pmod{21}\))

- The congruence \(6x \equiv 1 \pmod{21}\)

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

- Find all solutions to \(4x \equiv 5 \pmod{7}\)

  Set \(n\) since 7 is prime and \(7\) \(\neq 4\)
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 \( 2 = 4^{-1} \)

\[ \Rightarrow \text{ instead of } \text{"dividing both sides of } u_2 x \equiv 5 \text{ " by } 4 \text{ "} \]

\[ \text{"multiply both sides by } 2 \text{"} \]

\[ u_2 x = 5 \pmod{7} \]

\[ 2 \cdot u_2 x = 10 \equiv 5 \pmod{7} \]

\[ 8 x = 10 \pmod{7} \]

\[ x = 10 \pmod{7} \]

\[ x \equiv 3 \pmod{7} \]

and if \( x \equiv 3 \pmod{7} \)

then \( u_2 x \equiv 12 \equiv 5 \pmod{7} \)

so \[ u_2 x \equiv 5 \Rightarrow x \equiv 3 \pmod{7} \]

i.e.

\[ \{ 3 \} \cup \{ 5 \} \text{ is a set of solutions} \]
Prop. For any $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ (mod $n$) if $\gcd(a, n) \mid b$.

Proof. Let $d = \gcd(a, n)$.

$(\Rightarrow)$ Assume there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ (mod $n$), i.e., $\exists x, y \in \mathbb{Z}$ such that $ax + by = c$ (mod $n$).

i.e., $n \mid b - ac$

So, let $nk = b - ac$

i.e., $ak + nk = b$

So, since $d \mid c$ and $d \mid n$

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

we have

$dp + dq = b$

$= d(pl + qn) = b$

$i.e., d \mid b$

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

i.e., $\exists k \in \mathbb{Z}$ such that $d = b - ak$

By Bezout's Theorem, $\exists k, k' \in \mathbb{Z}$ such that $ak + nk' = d$

i.e., $a(k + nk') = d$

$= ake + nk'e = d = b$

i.e., $nk'e = b - a(k+e)$

i.e., $n \mid b - a(k + e)$

i.e., $a(k + e) = b \pmod{n} \Rightarrow k = k' \pmod{n}$
Ex's

1. There is a solution to $6x = 4 \pmod{8}$
   
   Why: $\gcd(6, 8) = 2$ and $2 \mid 4$
   
   Indeed, $x = 2$ works $\checkmark$

2. There is no solution to $4x = 3 \pmod{8}$
   
   Why: $\gcd(4, 8) = 4$
   
   and $4 \nmid 3$ $\checkmark$

Euclidean Algorithm

A lot 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 $\gcd(a, b) = \gcd(b, r)$

Proof: Let $d = \gcd(a, b)$

then $d = \gcd(b, r)$
Observe: \[ c = bq + r \quad \text{and} \quad d' \mid b \quad \text{and} \quad d' \mid r \quad \text{we knew} \quad d' \mid a \]
- so \[ d' \leq \gcd(a, b) \]

**Corollary:** By Bezout's Identity, s.t.: \[ rm + bn = d' \]
- but \[ r = a - bq \quad \text{so:} \]
  \[ (a - bq)m + bn = d' \]
- i.e. \[ cm + b(n - qn) = d' \]
- so \[ d' \] is a linear combo of \[ a, b \]

\[ \Rightarrow d' \geq d \]

so \[ d' = d \checkmark \]

This lemma allows us to find \( \gcd(a, b) \) by repeatedly "reducing by remainders."

**Thm (Euclidean Algorithm):**

Fix \( a, b \in \mathbb{N} \) with \( a \geq b \)
Define a finite decreasing sequence by
\[ r_0 = a \quad r_1 = b \]
\[ r_j = r_{j+1} q_{j+1} + r_{j+2} \]
where \( 0 \leq r_j < r_{j+1} \)
(iv) If \( r_n = 0 \) we define \( r_n \) as the last term.

Then: \( r_{n+1} = \text{gcd}(a,b) \)

Proof: Follows from Lemma but let's skip + see example.

Ex 1: Find \( \text{gcd}(68, 12) \)

\[ 68 = 12 \cdot 5 + 8 \]
\[ 12 = 8 \cdot 1 + 4 \]
\[ 8 = 4 \cdot 2 + 0 \]

\( \Rightarrow r_n = 0 \Rightarrow r_3 = 9 = \text{gcd}(68, 12) = \text{gcd}(12, 8) = \text{gcd}(8, 4) = 4 \)

Key: By Lemma:
\[ \text{gcd}(68, 12) = \text{gcd}(12, 8) = \text{gcd}(8, 4) = 4 \]
(v)

2. Find m, n \in \mathbb{Z} \text{ s.t. } 
\ 8m + 12n = 9

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

\[ 9 = 12 - 8 \cdot 1 \]
\[ = 12 - (68 - 12 \cdot 5) \cdot 1 \]
\[ = 12 - 68 \cdot 1 + 12 \cdot 5 \]
\[ = 12 \cdot 6 + 68 \cdot (-1) \]

So m = -1, n = 6 works!

This method of back substitution to find m, n is sometimes called the extended Euclid.

3. Find k, l \in \mathbb{Z} \text{ s.t. } 
\ 64k + 111l = 1

Solution: For this to be possible
must be that \text{gcd}(64, 111) = 1
Why do EA:

111 = 69\cdot1 + 47
- 69 = 47\cdot1 + 12
- 47 = 17\cdot2 + 13
- 17 = 13\cdot1 + 4
\rightarrow 17 = 4\cdot3 + 1 \leftarrow \text{gcd}(69, 111) \checkmark
\quad 4 = 4\cdot1 + 0

Now we go backwards from *:

1 = 17 - 4\cdot3 \quad \text{by} \quad q = 17 - 13\cdot1
\quad 1 = 17 - (17-13\cdot1)\cdot3
\quad = 17 - 17\cdot3 + 13\cdot3
\quad = 17 - 17\cdot3
\quad = 17(-3) + 13(4) \quad \text{but} \quad 17 = 47 - 17\cdot2
\quad = 17(-3) + (47-17\cdot2)(4)
\quad = 47(4) + 17(-3) + 17(-8)
\quad = 47(4) + 17(-11) \quad \text{but} \quad 17 = 69\cdot1 - 47
\quad = 47(4) + (69\cdot1 - 47)(-11)
\quad = 69(-11) + 47(4) + 47(11)
\quad = 69(-11) + 47(15) \quad \text{but} \quad 47
\quad = 69(-11) + (111-69\cdot1)(15) = 111 - 64\cdot1
\quad = 111(15) + 69(-11) + 64(-15)
\quad = 111(15) + 69(-11) + 64(-26)

So \( k = -26 \) and \( r = 15 \) work \( \checkmark \)