Alison Li

Recall: $[m]$ invertible in $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m, n$ coprime.
(avoid Euclid's algorithm).

Problem.
Find all invertible elements of $\mathbb{Z}/20\mathbb{Z}$, along with their inverses.
Invertible ones are $[11], [13], [17], [19]$.
Inverses appear on the same list.

$[1]^{-1} = [1]$
$[3]^{-1} = [7]$ since $3 \cdot 7 = 21 \equiv 1 \pmod{20}$
$[7]^{-1} = [3]$
$[9]^{-1} = [9]$ since $9^2 = 81 \equiv 1 \pmod{20}$
$[11]^{-1} = [11]$ since $11^2 = 121 \equiv 1 \pmod{20}$
$[13]^{-1} = [-7]^{-1} = [-3] = [17]$ since $(-7)(-3) = 21 \equiv 1$
$[17]^{-1} = [13]$
$[19]^{-1} = [-1]^{-1} = [-1] = [19]$ since $(-1)^2 = 1$.

Proposition.
If p is prime, then all non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ are invertible.
proof.
all $m = 1, 2, \dots, p-1$ have $\gcd(m, p) = 1$, hence invertible. $\square$

Solving Equations in $\mathbb{Z}/n\mathbb{Z}$ (i.e. mod n)

$\mathbb{Z}/n\mathbb{Z}$ has n elements so you can solve equations by trying all elements, 0 to $n-1$.

ex. Solve $[x]^2 = [x]$ in $\mathbb{Z}/6\mathbb{Z}$.
Try all 6 elements:

$[0]^2 = [0]$	$[3]^2 = [9] = [3]$ ✓
$[1]^2 = [1]$	$[4]^2 = [-2]^2 = [4]$ ✓
$[2]^2 = [4]$ ✗	$[5]^2 = [-1]^2 = [1]$ ✗

So, four solutions: $[0], [1], [3], [4]$.

ex. Solve $[x]^2 = [x]$ in $\mathbb{Z}/7\mathbb{Z}$.
$[0]^2 = [0]$ solution. If $[x] \neq [0]$ then $[x]$ invertible i.e. $[x]^{-1}$ exists, so
$[x]^2[x]^{-1} = [x][x]^{-1}$.
$[x] = [1]$ is the only solution.

Notation: If $[x]$ invertible, $[x]^{-n} = \underbrace{[x]^{-1} \cdots [x]^{-1}}_{= ([x]^{-1})^n}$ n times

ex. Find all $x \in \mathbb{Z}$ such that $x^2 \equiv x \pmod 6$.
We know $0, 1, 3, 4$ are solutions.
Hence, all solutions are of the form $6t$, $1 + 6t$, $3 + 6t$, $4 + 6t$ for $t \in \mathbb{Z}$.

ex. Solve $21x \equiv 17 \pmod{64}$.
Since $\gcd(21,64)=1$, 21 is invertible mod 64.
Euclid: $64 = 3\cdot 21 + 1 \to 1 = 64 - 3\cdot 21$.
So $[21]^{-1} = [-3]$.
Multiply by -3:

$$(-3)21x \equiv (-3)17 \quad (\text{mod } 64)$$
$$-63x \equiv -51 \quad (-63 = -1\cdot 64 + 1, \text{ so } -63 \equiv 1 \ (\text{mod } 64))$$
$$x \equiv 13 \quad (-51 = -1\cdot 64 + 13)$$

Application: Divisibility Rules

Divisible by 9 rule.
n is divisible by 9 $\Leftrightarrow$ sum of digits of n (base 10) divisible by 9.
proof.
In base 10:

$$n = d_0 10^0 + d_1 10^1 + d_2 10^2 + \cdots + d_k 10^k = \sum_{i=0}^{k} d_i 10^i.$$

Consider $\mathbb{Z}/9\mathbb{Z}$:

$$[n] = \left[\sum_{i=0}^{k} d_i 10^i\right] = \sum_{i=0}^{k}[d_i 10^i] = \sum_{i=0}^{k}[d_i][10]^i = \sum_{i=0}^{k}[d_i][1] = \sum_{i=0}^{k}[d_i] = \left[\sum_{i=0}^{k} d_i\right].$$

Hence, if $9 \mid n$, then $n \equiv 0 \pmod 9$, so
$\sum d_i \equiv 0 \pmod 9$ i.e. $9 \mid \sum d_i$.

Conversely, if $9 \mid \sum d_i$ then $[d_i] = [0]$.
So $[n] = [0]$, so $9 \mid n$.

Application: Check Digits

ISBN (for books) is a 10-digit number $d_{10} d_9 d_8 \cdots d_1$ assigned to a published book. Digits d_{10} to d_2 are used to identify books.
The last digit d_1 is chosen so that:

$$\sum_{i=1}^{10} i d_i \equiv 0 \pmod{11}.$$

d_1 is called 'check digit' (d_1 might need to be 10, symbol 'X' is used.
e.g. if $10d_{10} + 9d_9 + \cdots + 2d_2 \equiv 5 \pmod{11}$:
set $d_1 = 6$ so $(10d_{10} + 9d_9 + \cdots + 2d_2) + 6 \equiv 0 \pmod{11}$.

Prove that if $d_{10} \cdots d_1$ is a valid ISBN
(i.e. $\sum_{i=1}^{10} i d_i \equiv 0 \pmod{11}$), then:

(1) If any single digit is altered, the result is invalid (sum $\neq 0$).
(2) If two adjacent (different) digits are swapped, the result is invalid.

proof.
Let $c_{10} c_9 \cdots c_1$ be the new ISBN.
(changing original by either (1) or (2).)
(1) $c_i = d_i$ except some $c_k \neq d_k$, for some k.
By contradiction, assume $c_{10} \cdots c_1$ is valid i.e. $\sum i c_i \equiv 0 \pmod{11}$.
⋮

Alison Li

Then,

$$0 \equiv \sum_{i=1}^{10} i d_i - \sum_{i=1}^{10} i c_i \pmod{11}$$

$$0 \equiv k d_k - k c_k \equiv k(d_k - c_k).$$

In $\mathbb{Z}/11\mathbb{Z}$ (11 prime) so k invertible i.e. $km \equiv 1 \pmod{11}$ some m since $k, 11$ coprime. So,

$$0 \equiv mk(d_k - c_k) \equiv d_k - c_k \pmod{11}$$

$$0 \equiv d_k - c_k \rightarrow d_k \equiv c_k$$

but $d_k, c_k \in \{0, 1, \dots, 10\}$, contradicts $d_k \neq c_k$ so $c_{10} \cdots c_1$ invalid.

(2) Assume two adjacent digits, say d_k, d_{k+1} are swapped, so $c_i = d_i$, except $c_k = d_{k+1}$ and $c_{k+1} = d_k$.

By contradiction, assume $c_{10} \cdots c_1$ is valid, i.e. $\sum i c_i \equiv 0$.

Then,

$$0 \equiv \sum i d_i - \sum i c_i \equiv (k d_k + (k+1) d_{k+1}) - (k c_k + (k+1) c_{k+1}).$$

$$0 \equiv (k d_k + (k+1) d_{k+1}) - (k d_{k+1} + (k+1) d_k) \text{ by substitution of } c_k, c_{k+1}.$$

$$0 \equiv d_{k+1} - d_k \text{ so } d_k \equiv d_{k+1} \text{ (both in } \{0, 1, \dots, 10\})$$

but these are different digits by assumption (2).

Contradiction. So $c_{10} \cdots c_1$ invalid. $\square$

Fermat's Little Theorem and Applications

Lemma.

If p prime and $0 < k < p$ then $p \mid \binom{p}{k}$.

```
        1
      1 2 1
    1 3 3 1        → (3 choose k)
   1 4 6 4 1
 1 5 10 10 5 1     → (5 choose k)
```

proof.

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad \text{so} \quad p! = \binom{p}{k} k!(p-k)!$$

Hence,

$$p(p-1)! = \binom{p}{k} k! (p-k)!$$

So,

$$p \mid \binom{p}{k} (\underbrace{1 \cdot 2 \cdot 3 \cdot \cdots \cdot k}_{k!}) - (\underbrace{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-k)}_{(p-k)!})$$

Since p prime, p divides any of:

$$\binom{p}{k}, \overbrace{1, 2, 3, \dots, k}^{1 \text{ to } k}, \overbrace{1, 2, 3, \dots, p-k}^{1 \text{ to } p-k}$$

but p does not divide any of $1, 2, \dots, k$, $1, 2, \dots, p-k$ since $p > k$ and $p > (p-k)$. So $p \mid \binom{p}{k}$. $\square$

Corollary

If $x, y \in \mathbb{Z}$, p prime, then $(x+y)^p \equiv x^p + y^p \pmod{p}$.

proof.

$$(x+y)^p = \binom{p}{0} x^0 y^p + \binom{p}{1} x^1 y^{p-1} + \dots + \binom{p}{p-1} x^{p-1} y^1 + \binom{p}{p} x^p y^0 \text{ by binomial theorem.}$$

$$\equiv y^p + 0 + \dots + 0 + x^p \pmod{p}.$$

Since $p \mid \binom{p}{k}$ $0 < k < p$ (each of the coefficients are divisible by p). $\square$