Recall: Basic Arithmetic

- Modular Arithmetic
- Chinese Remainder
- Towards Algebra

Comment 1

So far, we have dealt with various aspects of elementary combinatorics:

- induction
- counting
- graphs
- (finite) probability
- (finite) games

In the next few weeks we deal with algebra, then with computability.

Comment 2

You know everything in this first section.

Instead of falling asleep, think about how you might actually prove all these assertions.

In this case, a real proof should be based on Peano arithmetic: take the basic laws of addition and multiplication, plus a suitable form of induction. Figure out how to formalize induction on the integers.

Comment 3

Next week you will see a more elegant and mathematically more useful way to explain what is going on: actual algebra.

Alas, high levels of abstraction are utterly useless without a solid grounding in actual examples. This week we provide some concrete examples, next week we talk about the corresponding abstractions:

- groups
- rings and fields

Needless to say, this is also the way the area developed historically. Understanding modern math without history is very difficult.

Total Recall: Divisibility

For $a, b \in \mathbb{Z}$, $a$ divides $b$ iff $\exists c \in \mathbb{Z}(a \cdot c = b)$.

This is usually written $a \mid b$.

Proposition

Note that $1, -1 \mid a$ and $a \mid 0$. Divisibility is reflexive, transitive and almost antisymmetric.

Lemma (Linear Combinations)

If $d \mid a$ and $d \mid b$ then $d \mid (xa + yb)$ for all $x, y \in \mathbb{Z}$. 
Theorem (Division Theorem)
Let $b$ be positive, and $a$ an arbitrary integer. Then there exist integers $q$ and $r$ such that
\[ a = q \cdot b + r, \text{ where } 0 \leq r < b. \]
Moreover, the numbers $q$ and $r$ are uniquely determined (quotient and remainder).

In the literature this is often called the “Division Algorithm,” though no algorithm is given.

Notation:
\[ r = a \mod b \quad \text{remainder} \]
\[ q = a \div b \quad \text{quotient} \]

Primes

$p > 1$ is prime iff its only positive divisors are 1 and $p$.

Lemma
For every $n \geq 2$ there is a prime $p$ such that $p \mid n$.

Theorem
There are infinitely many primes.

Lemma
If $p$ is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Sample Proof

The last lemma requires a forward link to GCD, see below.

Let $d = \gcd(a, p)$.

If $d = p$ then clearly $d$ divides $a$.

But otherwise $d = 1$, hence $xa + yp = 1$ for some integers $x$ and $y$.

It follows that $xab + ypb = b$ and $p$ divides $b$.

\[ \square \]

The Fundamental Theorem

Let $n \geq 2$. Then there exist distinct primes $p_1, \ldots, p_k$ such that
\[ n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \]
where $e_i > 0$. The decomposition is unique up to order.

Proof.
Strong induction and the last lemma.

But beware, finding this prime decomposition is very hard. It is exceedingly useful conceptually, but algorithmically there are issues.

GCD and Euclidean Algorithm

The greatest common divisor is defined by
\[ \gcd(a, b) = \max \{ d \mid d \text{ divides } a, b \} \]
a and $b$ are coprime (relatively prime) iff $\gcd(a, b) = 1$.

A look at the GCD function produces an algorithm to compute it.

Lemma
- $\gcd(x, 0) = x$
- $\gcd(x, y) = \gcd(y, x)$
- $\gcd(x, y) = \gcd(y, x \mod y)$

Example

Typical run: $a = 4234$ and $b = 4693286$.

\[ 4234 = 0 \cdot 4693286 + 4234 \]
\[ 4693286 = 1108 \cdot 4234 + 2014 \]
\[ 4234 = 2 \cdot 2014 + 206 \]
\[ 2014 = 9 \cdot 206 + 160 \]
\[ 206 = 1 \cdot 160 + 46 \]
\[ 160 = 3 \cdot 46 + 22 \]
\[ 46 = 2 \cdot 22 + 2 \]
\[ 22 = 11 \cdot 2 + 0 \]

The table is a (clumsy) proof that $\gcd(4234, 4693286) = 2$. 
The last example suggests to take a closer look at linear combinations
\[ c = x \cdot a + y \cdot b \]
where \( x, y \in \mathbb{Z} \).

Obviously \( c \) is divisible by \( \gcd(a, b) \).

More interestingly, one could run through the equations above backwards and write \( 2 = \gcd(a, b) \) as a linear combination of \( a \) and \( b \):
\[ \gcd(a, b) = 2 = 205068 \cdot a - 185 \cdot b \]
A simple induction shows that
\[ r_i = a \cdot x_i + b \cdot y_i. \]

We have
\[
\begin{array}{ccc}
q_i & r_i & x_i & y_i \\
-1 & 1233 & 1 & 0 \\
-1 & 1000 & 0 & 1 \\
1 & 233 & 1 & -1 \\
4 & 68 & -4 & 5 \\
3 & 29 & 13 & -16 \\
2 & 10 & -30 & 37 \\
2 & 9 & 73 & -90 \\
1 & 1 & -103 & 127 \\
9 & 0 & 1000 & -1233 \\
\end{array}
\]

We have
\[
-103 \cdot 1233 + 127 \cdot 1000 = 1 = \gcd(1233, 1000)
\]

We can also think of
\[ a \cdot x + b \cdot y = c \]
as an equation, we want solutions for \( x \) and \( y \).

Again, we clearly need \( d = \gcd(a, b) \mid c \) for any solution to exist.

We can divide by the GCD and use the extended Euclidean algorithm as before.

But note that the solution is not unique: for any solution \((x_0, y_0)\) we get infinitely many other solutions of the form
\[ (x_0 + tb/d, y_0 - ta/d) \]
where \( t \in \mathbb{Z} \). In fact, these are all the solutions.

Definition
Let \( p \) prime. The \( p \)-adic valuation of an integer \( n \neq 0 \) is the largest \( e \) such that \( p^e \) divides \( n \), in symbols \( \nu_p(n) \); we set \( \nu_p(0) = \infty \).

\[
\nu_p(ab) = \nu_p(a) + \nu_p(b)
\]

\[ a \mid b \iff \forall p \left( \nu_p(a) \leq \nu_p(b) \right) \]

\[
\gcd(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}
\]

The last formula does not yield an efficient way to compute \( \gcd \)'s.
The natural numbers with division \( \langle \mathbb{N}, | \rangle \) form a so-called lattice: a partial order where any two elements have a join (supremum) and a meet (infimum).

The join is the least common multiple, the meet the greatest common divisor.

If you prefer, you can think of a structure \( \langle A, \sqcup, \sqcap \rangle \) where \( \sqcup \) and \( \sqcap \) are associative and commutative absorption holds:

\[
x \sqcup (x \sqcap y) = x \quad x \sqcap (x \sqcup y) = x
\]

---

**Exercise**

Verify that \( \langle \mathbb{N}, \text{lcm}, \gcd \rangle \) really forms lattice.

**Exercise**

How are lcm and gcd expressed in the picture of the divisor lattice of 30?

**Exercise**

How is the structure of prime divisors of 148176 = \( 2^43^37^3 \) expressed in the picture of the divisor lattice?

---

**Odds and Evens**

Suppose we have a polynomial with integer coefficients

\[
p(x) = a \cdot x^3 + b \cdot x^2 + c \cdot x + d.
\]

Assume that both \( p(0) \) and \( p(1) \) are odd.

**Claim**

*For all integers \( x \), \( p(x) \neq 0 \).*

To see why, first note that \( d = p(0) \) and \( a + b + c + d = p(1) \) are odd.

**Even/Odd arithmetic:**

<table>
<thead>
<tr>
<th>+</th>
<th>even</th>
<th>odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>even</td>
<td>even</td>
<td>odd</td>
</tr>
<tr>
<td>odd</td>
<td>odd</td>
<td>even</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-</th>
<th>even</th>
<th>odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>even</td>
<td>even</td>
<td>odd</td>
</tr>
<tr>
<td>odd</td>
<td>odd</td>
<td>even</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*</th>
<th>even</th>
<th>odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>even</td>
<td>even</td>
<td>odd</td>
</tr>
<tr>
<td>odd</td>
<td>odd</td>
<td>even</td>
</tr>
</tbody>
</table>
Hence $n$ even (odd) implies $n^k$ even (odd) for all $k \geq 1$.

**Case 1:** So for even $x$ we get

$$p(x) = a \cdot \text{even} + b \cdot \text{even} + c \cdot \text{even} + \text{odd} = \text{odd}$$

so that in particular $p(x) \neq 0$.

**Case 2:** For odd $x$ we have

$$p(x) = a \cdot \text{odd} + b \cdot \text{odd} + c \cdot \text{odd} + \text{odd}.$$ 

But $a + b + c$ must be even, so either 0 or 2 of these coefficients must be odd.

In both cases $p(x)$ is odd, and so not equal to 0.

---

**Modular Arithmetic, Courtesy C. F. Gauss**

Recall from equivalence relations: for $m \geq 0$, $x$ is congruent to $y$ modulo $m$

$$x \equiv y \iff m \text{ divides } x - y$$

is an equivalence relation.

**Notation:** $x \equiv y \pmod{m}$ or $x \equiv y \pmod{m}$.

**Crucial Point:** we can define arithmetic on the equivalence classes to get a structure $\mathbb{Z}_m$ as opposed to $\mathbb{Z}$:

$$[x] + [y] = [x + y]$$

$$[x] \cdot [y] = [x \cdot y]$$

We obtain modular numbers.

---

**Representatives and Notation**

A notation like $[x]$ or $[x]_m$ or $[x]_{\mathbb{Z}_m}$ for modular numbers is perfectly correct but fatally clumsy. Likewise for $+_m$ or $+_{\mathbb{Z}_m}$.

To keep notation simple, we will usually ignore the brackets and write $x$ instead of $[x]$. And we write $+ \text{ and } \cdot$ for addition and multiplication of modular numbers.

So, we write $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ and sometimes think of $\mathbb{Z}_m \subseteq \mathbb{Z}$.

This is the canonical way of choosing representatives, but note that there are other possibilities. For example, for $m = 2k + 1$ we could also use

$$-k, -k + 1, \ldots, -1, 0, 1, \ldots, k - 1, k$$
There is a very important idea hiding here: equivalence relations that are compatible with arithmetic (here: on modular numbers).

Suppose $\rho$ is an equivalence relation on $\mathbb{Z}$. $\rho$ is a congruence iff

$$x = x' \pmod{m} \quad \text{and} \quad y = y' \pmod{m}$$

implies

$$x + y = x' + y' \pmod{m}$$

and

$$x \cdot y = x' \cdot y' \pmod{m}$$

This is a huge restriction compared to arbitrary equivalence relations. There are uncountably many equivalence relations on $\mathbb{Z}$, but we know all the congruences: the Gaussian relations mod $m$.

**Exercise**

Prove that any congruence on the integers is already of the form $\pmod{m}$.

Think of $\mod m$ as a function from $\mathbb{Z}$ to $\mathbb{Z}_m \subseteq \mathbb{Z}$.

Then we have

$$(x + y) \mod m = ((x \mod m) + (y \mod m)) \mod m$$

and

$$(x \cdot y) \mod m = ((x \mod m) \cdot (y \mod m)) \mod m$$

Note that the double application of $\mod m$ on the right is clumsy, we’ll see a better way in a while (homomorphisms).

A clock (which functions accurately) shows the hour hand positioned at a minute mark, and the the minute hand two marks away. What time is it?

Really have 60 possible positions. Equations:

$$m = h \pm 2 \pmod{60}$$

$$m = 12h \pmod{60}$$

By exploiting the congruence properties it follows that

$$11h = \pm 2 \pmod{60}$$

multiply by 11:

$$h = \pm 22 \pmod{60}$$

It’s 4:24 or 7:36.

First an important special case.

**Lemma**

The equation

$$a \cdot x = 1 \pmod{m}$$

has a solution if, and only if, $a$ and $m$ are coprime. The solution is unique modulo $m$, if it exists.

**Proof.**

A solution means that $ax - 1 = qm$, so $a$ and $m$ must be coprime.

In the opposite direction use the extended Euclidean algorithm to compute cofactors $ax + my = 1$. 

In particular when $a$ and $m$ are coprime we can simply drop the $a$.

**Exercise**

Use $p$-adic valuations to prove the proposition.
### Multiplicative Inverses

The situation in the lemma is very important.

The solution $x$ such that $ax = 1 \pmod{m}$ is called the **multiplicative inverse** of $a$ (modulo $m$).

Notation: $a^{-1} \pmod{m}$.

**Example**

$m = 11$.

<table>
<thead>
<tr>
<th>$m^{-1}$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>9</td>
<td>2</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

Note that $10 = 10^{-1}$ (no surprise, really: $10 = -1$).

So $1/2 = 6 \pmod{11}$.

### Euler’s Totient Function

The collection of all modular numbers that have a multiplicative inverse is usually written $\mathbb{Z}^*_m$ and called the **multiplicative subgroup** (see next week).

**Definition**

$$\mathbb{Z}^*_m = \{ a \in \mathbb{Z}_m \mid \gcd(a, m) = 1 \}$$

**Definition (Euler’s Totient Function)**

The cardinality of $\mathbb{Z}^*_m$ is written $\varphi(m)$.

Here are the first few values of $\varphi$:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\varphi(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>18</td>
<td>12</td>
</tr>
<tr>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>21</td>
<td>16</td>
</tr>
<tr>
<td>22</td>
<td>20</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>24</td>
<td>12</td>
</tr>
<tr>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>26</td>
<td>24</td>
</tr>
<tr>
<td>27</td>
<td>24</td>
</tr>
<tr>
<td>28</td>
<td>20</td>
</tr>
<tr>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>30</td>
<td>16</td>
</tr>
<tr>
<td>31</td>
<td>30</td>
</tr>
<tr>
<td>32</td>
<td>24</td>
</tr>
<tr>
<td>33</td>
<td>24</td>
</tr>
<tr>
<td>34</td>
<td>32</td>
</tr>
<tr>
<td>35</td>
<td>32</td>
</tr>
<tr>
<td>36</td>
<td>24</td>
</tr>
<tr>
<td>37</td>
<td>36</td>
</tr>
<tr>
<td>38</td>
<td>32</td>
</tr>
<tr>
<td>39</td>
<td>32</td>
</tr>
<tr>
<td>40</td>
<td>36</td>
</tr>
<tr>
<td>41</td>
<td>40</td>
</tr>
<tr>
<td>42</td>
<td>32</td>
</tr>
</tbody>
</table>

Looks complicated.

Note that we can compute $\varphi(n)$ if we know the prime factorization of $n$:

- For $p$ prime $\varphi(p) = p - 1$ and $\varphi(p^k) = (p - 1)p^{k-1}$.
- For $m$ and $n$ coprime, $\varphi(mn) = \varphi(m)\varphi(n)$.

We will see an elegant proof of the second claim later.

### Inhomogeneous Equations, II

**Lemma**

In the general case

$$a \cdot x = c \pmod{m}$$

we have a solution if, and only if, $\gcd(a, m)$ divides $c$.

Moreover, the number of solutions is $\gcd(a, m)$.

**Exercise**

Prove the general case.
Recall from Iteration

Consider the additive function
\[ \alpha : \mathbb{Z}_m \rightarrow \mathbb{Z}_m \]
\[ x \mapsto x + s \mod m \]

Clearly \( \alpha \) is injective, so the orbits are all periodic (plain cycles).

Moreover, since \( \alpha(x) + y = \alpha(x + y) \mod m \) all the cycles are just rotations of each other and it suffices to understand \( \text{orb}(0, \alpha) \).

So we need the least \( k > 0 \) such that \( ks = 0 \mod m \).

Let \( d = \text{gcd}(s, m) \). Then clearly \( k = m/d \).

Proposition
\( \alpha \) has \( \gcd(s, m) \) distinct orbits, each of length \( m/\gcd(s, m) \).

Wilson’s Theorem

Theorem (Wilson’s Theorem)
\( p \) is prime if, and only if, \( (p-1)! \equiv -1 \mod p \).

Proof.
First assume \( p \) is prime, wlog \( p > 2 \). We can pair off \( a \in \mathbb{Z}_p^* \) and \( a^{-1} \in \mathbb{Z}_p^* \).
\( a \) and \( a^{-1} \) are always distinct except in the case \( a = \pm 1 \): the quadratic equation \( x^2 = 1 \mod p \) has at most two solutions since \( x^2 - 1 = (x+1)(x-1) \).

For the opposite direction assume \( p \) fails to be prime, say, \( ab = p \) for \( 1 < a < b < p \). But then \( (p-1)! \) and \( p \) are not coprime whereas \(-1\) and \( p \) are coprime, contradiction.
Chinese Remainder

Theorem (Fermat’s Little Theorem)

If $p$ is prime and coprime to $a$, then $a^{p-1} = 1 \pmod{p}$.

Proof.

Consider the map $f : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$, $f(x) = ax$.

$f$ is a bijection, so

$$a^{p-1} \prod_{x \in \mathbb{Z}_p^*} x = \prod_{x \in \mathbb{Z}_p^*} ax = \prod_{x \in \mathbb{Z}_p^*} f(x) = \prod_{x \in \mathbb{Z}_p^*} x \quad \pmod{p}$$

Since $\varphi(p) = p - 1$, done.

We will see a stronger version of this in our discussion of groups.

Little Fermat

Theorem (Fermat’s Little Theorem)

If $p$ is prime and coprime to $a$, then $a^{p-1} = 1 \pmod{p}$.

Proof.

Let $m_1 = 3$ and $m_2 = 5$, so $m = 15$.

Here is the canonical map $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$, $f(x) = (x \pmod{3}, x \pmod{5})$.

<table>
<thead>
<tr>
<th>$x$ (mod 3)</th>
<th>$x$ (mod 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
</tr>
</tbody>
</table>

By table lookup, the solution to $x = 2 \pmod{3}$, $x = 1 \pmod{5}$ is $x = f^{-1}(2, 1) = 11$.

Multiple Linear Equations

How about multiple equations with several moduli:

$$a_i x = b_i \pmod{m_i} \quad \text{where } i = 1, \ldots, n$$

We can simplify this system a little: for a solution to exist we need that $\gcd(a_i, m_i)$ divides $b_i$.

So we get an equivalent equation $a_i' x = b_i' \pmod{m_i'}$ where $a_i'$ and $m_i'$ are coprime.

But that is equivalent to $x = c_i \pmod{m_i'}$ for some appropriate $c_i$.

Proof

To see this, suppose $f(x) = f(x')$, where $0 \leq x \leq x' < m$.

Then

$$x' - x = q_1 m_1 = q_2 m_2.$$ 

But $m_1$ and $m_2$ are coprime, so $m_1 | x' - x$ and therefore $x = x'$.

Since domain and codomain of $f$ both have cardinality $m$, $f$ must be a bijection by General Abstract Nonsense.

Hence we can solve $x = a \pmod{m_1}$ and $x = b \pmod{m_2}$: let

$$x = f^{-1}(a, b)$$

Great. But how do we find the $x$ computationally?

Multiple Linear Equations, II

So let’s only consider

$$x = a_i \pmod{m_i} \quad i = 1, \ldots, n$$

Tricky in general, but for coprime moduli easy. We only consider $n = 2$.

Let $m = m_1 m_2$ and define the function

$$f : \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}, \quad f(x) = (x \pmod{m_1}, x \pmod{m_2})$$

Claim

$f$ is injective and hence bijective.

CRT Example

Let $m_1 = 3$ and $m_2 = 5$, so $m = 15$.

Here is the canonical map $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$, $f(x) = (x \pmod{3}, x \pmod{5})$.

<table>
<thead>
<tr>
<th>$x$ (mod 3)</th>
<th>$x$ (mod 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
</tr>
</tbody>
</table>

By table lookup, the solution to $x = 2 \pmod{3}$, $x = 1 \pmod{5}$ is $x = f^{-1}(2, 1) = 11$. 

Recall: Basic Arithmetic

Modular Arithmetic

Chinese Remainder

Towards Algebra
A better method is to use the EEA. Compute the cofactors:
\[ \alpha m_1 + \beta m_2 = 1 \]
Then
\[ f(\alpha m_1) = (0,1) \]
\[ f(\beta m_2) = (1,0) \]
whence
\[ f(b\alpha m_1 + a\beta m_2) = (a,b) \]
So the solution is
\[ x = b \cdot \alpha m_1 + a \cdot \beta m_2. \]

As we have seen, the solution to
\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 1 \pmod{5} \]
is \[ x = 11. \]

Here is the computationally superior solution: determine cofactors
\[ (-3) \cdot 3 + 2 \cdot 5 = 1 \]
which produce a solution
\[ x = 1 \cdot (-3) \cdot 3 + 2 \cdot 2 \cdot 5 = 11 \]

Our result also holds for more than 2 equations (and is very old).

**Theorem (CRT)**
Let \( m_i, i = 1, \ldots, n \) be pairwise coprime. Then the equations
\[ x = a_i \pmod{m_i} \quad i = 1, \ldots, n \]
have a unique solution in \( \mathbb{Z}_{m_1 m_2 \ldots m_n} \).

This follows from repeated application of the solution for \( n = 2 \) since \( m_1 \) and \( m_2 \ldots m_2 \) are also coprime.

How do we compute the solution for \( n > 2 \)? We could use the method for \( n = 2 \) recursively, but that is a bit tedious. Here is a better way.

Define
\[ c_i = m/m_i \]
so that \( c_i \equiv 0 \pmod{m_j}, i \neq j \), but \( c_i \) and \( m_i \) are coprime. Use EEA to find inverses
\[ \alpha_i c_i \equiv 1 \pmod{m_i} \]
Then
\[ x = a_1 \alpha_1 c_1 + a_2 \alpha_2 c_2 + \ldots a_n \alpha_n c_n \quad \pmod{m} \]

A bored bank clerk has a big pile of one-dollar bills in front of him. He rearranges the bills first in groups of 2, then 3, and 4, 5, 6, 7, 8, 9, 10 and 11. In all cases except the last, one bill is left over. In the last case, no bill is left over.

How big is the original pile?

Note that we cannot use the CRT directly: the moduli are not coprime.

But \( x = 1 \mod 8 \) implies \( x = 1 \mod 4 \) and \( x = 1 \mod 2 \).

Moreover, \( x = 1 \mod 9 \) implies \( x = 1 \mod 3 \). And both together imply \( x = 1 \mod 6 \).

Similarly we can drop the condition modulo 10.
In general, a solution may exist even if some of the moduli are not coprime. This is expressed in the following generalization.

**Theorem (Generalized CRT)**

The equations

\[ x = a_i \pmod{m_i} \quad i = 1, \ldots, n \]

have a solution if, and only if, for all \( i \neq j \):

\[ a_i = a_j \pmod{\gcd(m_i, m_j)} \]

The solution is unique modulo \( m = \text{lcm}(m_1, m_2, \ldots, m_n) \).

---

**A Closer Look**

In the CRT example from above we had

\[ 11 + 8 = 4 \mod 15 \quad (2, 1) + (2, 3) = (1, 4) \mod (3, 5) \]
\[ 11 \cdot 8 = 13 \mod 15 \quad (2, 1) \cdot (2, 3) = (1, 3) \mod (3, 5) \]

It looks like

\[ f(x + y) = f(x) + f(y) \]
\[ f(x \cdot y) = f(x) \cdot f(y) \]

Here we are joyfully abusing notation, we do not distinguish between the \(+\) operation in \( \mathbb{Z}_{15} \) and its counterpart in \( \mathbb{Z}_3 \times \mathbb{Z}_5 \).

---

**Logarithms**

Here is the classic historical example of such a map:

\[ \log : \mathbb{R}^+ \rightarrow \mathbb{R} \]

which translates multiplication into addition (next week: a group isomorphism from \( (\mathbb{R}^+, \cdot, 1) \) to \( (\mathbb{R}, +, 0) \)).

We can compute products of (positive) reals by

\[ x \cdot y = e^{\log x + \log y} \]

Makes a huge difference: \( O(k) \) plus table lookup rather than \( O(k^2) \) where \( k \) is the number of decimal digits.

Of course, we have to compute a logarithm table first—but only once. It took John Napier some 20 years to construct such a table in the early 1600s.