Solving integer congruences

- We want to think about solving congruences "for x" just like solving equations "for x".
- The general form is

$$mx \equiv a \pmod{n}$$

  where m, a, and n are given.
- The problem is that you can't "divide through by m" all the time. If a is a multiple of m, a/m will be an integer, but – for example –

$$4x \equiv 1 \pmod{6}$$

  has no (integer) solution x.
- Under what conditions will there be a unique solution for x?

Multiplicative inverses mod n

- First of all, consider the congruence

$$mx \equiv 1 \bmod n.$$

- Can there be an integer x that "acts like" $1/m$?
- An x that satisfies this congruence is called a multiplicative inverse of m modulo n.
- Sometimes there is no such thing. For the congruence $4x \equiv 1 \bmod 6$ there isn't any "1/4" in the mod 6 number system.
- Why? A solution x has to obey the definition $4x = 1 + 6k$ for an integer k. But for any integers x, k, the number $4x$ is even, and $1 + 6k$ is odd.
- It turns out that the problem here is that 4 and 6 have a common divisor (2) greater than 1.

Existence and non-existence of multiplicative inverses

- If $\gcd(m, n) > 1$, then there is no integer solution to $mx \equiv 1 \bmod n$.
- The reason is that an integer solution x has to satisfy

$$mx = 1 + nk \text{ for some } k \in \mathbb{Z}.$$

  But mx is a multiple of $\gcd(m, n)$ and so is nk. If we take the remainders mod the gcd, we get 0 on the left and 1 on the right.
- However, it's fortunate that when $gcd(m, n) = 1$ there is always a multiplicative inverse mod n, and a unique such in $\mathbb{Z}_n$.
- This case is so important that when $\gcd(m, n) = 1$ we say that m and n are relatively prime.

The $sm + tn$ theorem

- **Theorem** *For non-negative integers m and n, there are "integer coefficients" s and t such that*

$$\gcd(m, n) = sm + tn.$$

- **Corollary** *When m and n are relatively prime, there is always a solution x to $mx \equiv 1 \pmod{n}$.*

  Proof (of the corollary): By the theorem, there are integers s and t such that $sm + tn = 1$. Thus, $sm = 1 - tn$, so $sm = ms$ differs from 1 by a multiple of n, which by definition means $ms \equiv 1 \pmod{n}$. Therefore s is the desired solution x.

- By looking at the proof of the theorem, using strong induction, we can obtain a new recursive version (just as fast) of Euclid's algorithm which – given m and n – will return the required coefficients s and t.

Proof of the $sm + tn$ theorem

- We prove the following formal statement by strong induction on n:

$$(\forall n \in \mathbb{N})[(\forall m \in \mathbb{N}^+)(\exists s, t \in \mathbb{Z})(\gcd(m, n) = sm + tn)].$$

- *Basis:* $n = 0$. Then $gcd(m, 0) = m$. We may choose $s = 1$ and $t = 0$ to get $m = 1 \cdot m + 0 \cdot n$.

- *Induction step:* Assume for all $0 \leq r < n$ that for any m

$$\gcd(m, r) = s'm + t'r$$

for some integers s', t'. We have to show that there are integers s, t with $\gcd(m, n) = sm + tn$.

By the lemma showing correctness of Euclid's algorithm,

$$\gcd(m, n) = \gcd(n, m \bmod n).$$

Since $m \bmod n < n$, we can use $m \bmod n$ as r in the inductive hypothesis, and we can replace m by n there, too, because the IH holds for *any* m. This gives us – using the IH –

$$\gcd(m, m \bmod n) = s'n + t'(m \bmod n)$$

for some integers $s', t' \in \mathbb{Z}$. Furthermore, $m = qn + r$, so that

$$\gcd(m, n) = \gcd(n, r) = s'n + t'r = s'n + t'(m - qn) = t'm + (s' - t'q)n$$

so we can take $s = t'$ and $t = s' - t'q = s' - t' \cdot (m \text{ div } n)$. This finishes the inductive step.

The recursive version of Euclid

- Recall Euclid's algorithm:

```
function gcd(m:ℕ⁺; n:ℕ);
{
(a, b) := (m, n);
while b != 0 do % gcd(a,b) = gcd(m,n)
(a,b) := (b, a mod b);
gcd(m,n) := a
}
```

- This while-program can be written as a recursive one:

```
function gcd(m:ℕ⁺; n:ℕ);
{
if n = 0 then gcd(m,n) := m;
else gcd(m,n) := gcd(n, m mod n);
}
```

- We'll add some local variables which will compute the s and t guaranteed by the $sm + tn$ theorem .

Extended GCD

- Recall the last step in the inductive proof of the $sm + tn$ theorem:

$$\gcd(m,n) = \gcd(n,r) = s'n + t'r = s'n + t'(m - qn) = t'm + (s' - t'q)n$$

  so we can take $s = t'$ and $t = s' - t'q = s' - t' \cdot (m \text{ div } n)$.

- This allows us to create local variables `d,s,t` where `d` stands for the gcd, and `s,t` are the required coefficients:

```
procedure egcd(m:ℕ⁺; n:ℕ);
{
if n = 0 return (m,1,0);
else { (d', s', t') := egcd(n, m mod n);
(d, s, t) := (d', t', s' - t'* (m div n));
return (d,s,t);}
}
```

- This allows us to calculate the s and t, and also to calculate multiplicative inverses.

Example EGCD calculation

- ```
  procedure egcd(m:ℕ+; n:ℕ);
  {
  if n = 0 return (m,1,0);
  else { (d', s', t') := egcd(n, m mod n);
  (d, s, t) := (d', t', s' - t'* (m div n));
  return (d,s,t);}
  }
  ```
- Let's use this algorithm to calculate gcd(99, 78) and s, t such that $\gcd(99, 78) = s \cdot 99 + t \cdot 78$. We can use the following array.

`egcd` calls	quotient q	(d, s, t)	$t = s' - t' \cdot q$
(99,78)	1	(3, -11, 14)	14 = 3 - (-11)* 1
(78,21)	3	(3, 3, -11)	-11 = -2 - 3*3
(21,15)	1	(3, -2, 3)	3 = 1 - (-2)*1
(15,6)	2	(3, 1, -2)	-2 = 0 - 1* 2
(6,3)	2	(3, 0, 1)	1 = 1 - 0*2
(3,0)		(3, 1, 0)	
fill down	fill down	fill up	fill up

We fill the first two columns down and then the second two columns up.
  ```

Example: finding a multiplicative inverse

- Solve $33x \equiv 1 \pmod{26}$.
- Soilution: 33 and 26 are relatively prime. We first find s and t such that

$$s \cdot 33 + t \cdot 26 = 1.$$

- I cheated here, because $33 \cdot 3 = 99$ and $26 \cdot 3 = 78$, and from the last slide,

$$3 = (-11) \cdot 99 + 14 \cdot 78$$

  so dividing out by 3

$$1 = (-11) \cdot 33 + 14 \cdot 26.$$

- So $(-11) \cdot 33 \equiv 1 \pmod{26}$, and therefore we may take $x = -11$. It turns out that any other solution y is congruent to -11 mod 26, so you can add 26 to -11, for the least non-negative solution 15.

Uniqueness of multiplicative inverses

- We now know that if m and n are relatively prime, then there is a solution x to $mx \equiv 1 \pmod{n}$.

- What are all of the solutions? Clearly we can add any multiple of n to the first x we find, to get other solutions. Are these the only other ones?

- To answer this, let y be another solution, so that

$$my \equiv 1 \pmod{n}.$$

  Therefore, $my \equiv mx \pmod{n}$, so that $n \mid (my - mx) = m(y - x)$.

- Since m and n are relatively prime, no divisor of n can divide m. Therefore all divisors of n divide $y - x$, which means that $y - x$ is a multiple of n. Therefore,

$$y \equiv x \pmod{n}$$

  and we have found all solutions.

- This means that if you find a solution x, just calculate $x \bmod n$ to get the only solution in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. That's because of the partition property of $\equiv \pmod{n}$.

The Chinese Remainder Theorem: An application of multiplicative inverses

- The Chinese mathematician Sun-Tsu (1st cent.) posed the following problem: There are fewer than 105 people in a local warlord's army. Let x be this number. I notice that

$$\begin{aligned} x \bmod 3 &= 2 \\ x \bmod 5 &= 3 \\ x \bmod 7 &= 2 \end{aligned}$$

  Can you determine x?

- Notice $3 \cdot 5 \cdot 7 = 105$.
- Not to keep you in suspense, the only possibility is $x = 23$.

Chinese Remainder Theorem: formal statement

- **Theorem** *Given moduli* $m_1, \ldots, m_k$ *relatively prime in pairs, let* M *be the product* $m_1 \cdot \cdots \cdot m_k$. *Then for given* $a_1, \ldots, a_k$ *there is a unique* x *in* $\mathbb{Z}_M$ *such that*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

- *Proof.* First we show existence. For $1 \le j \le k$ put $M_j = M/m_j$. Then $\gcd(m_j, M_j) = 1$ by the hypothesis. Solve the k congruences

$$M_j \cdot y_j \equiv 1 \pmod{m_j}$$

and then set

$$x = \sum_{j=1}^{k} a_j \cdot M_j \cdot y_j.$$

We claim $x \bmod M$ is the required solution. To see this, fix $j \le k$. Note that for $i \ne j$, $(a_i \cdot M_i \cdot y_i) \bmod m_i = 0$. This is because for $i \ne j$, we have $M_i \equiv 0 \pmod{m_j}$. We also have $a_j \cdot M_j \cdot y_j \equiv a_j$ modulo m_j, because $M_j y_j \equiv 1$ modulo m_j. Therefore for each j

$$x \equiv 0 + \cdots + a_j + \cdots + 0 = a_j \pmod{m_j}$$

So x satisfies the given congruences, and then so does $x \bmod M$, because each $m_j \mid M$.

Example: Sun-Tsu's problem

- Given

$$
\begin{aligned}
x \bmod 3 &= 2 \\
x \bmod 5 &= 3 \\
x \bmod 7 &= 2
\end{aligned}
$$

  we have $M = 3 \cdot 5 \cdot 7$. Therefore $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, and $M_3 = 105/7 = 15$.

- We solve the three congruences

$$
\begin{aligned}
35y_1 &\equiv 1 \pmod 3 \\
21y_2 &\equiv 1 \pmod 5 \\
15y_3 &\equiv 1 \pmod 7
\end{aligned}
$$

  getting $y_1 = 2, y_2 = 1$, and $y_3 = 1$. Then $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 20 = 233$.

- We take $233 \bmod 105 = 23$.

The Chinese Remainder Theorem: uniqueness

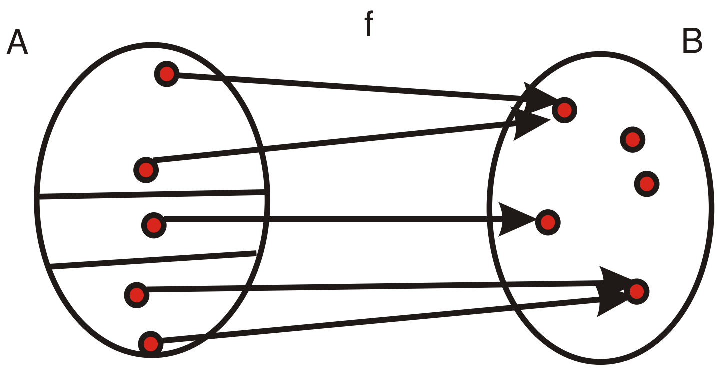
- This is really interesting! It's a consequence of a fundamental fact about functions on finite sets.

- **Lemma** *Let A and B be finite sets with the same number n of elements. If $f : A \to B$ is onto, then f is one-to-one.*

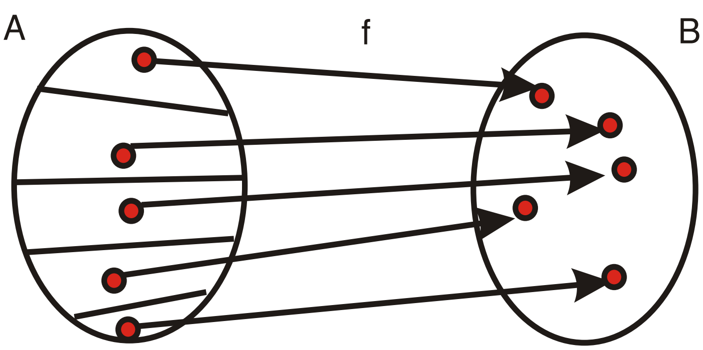
- *Proof:* Since f is onto, the sets $\{x \in A \mid f(x) = b\}$, as b ranges through B, form a partition of A. Every element of A is in exactly one of these sets. There are n sets in the partition, because B has n elements. But there are also n elements of A. Therefore each set in the partition is a singleton, because if you have n letters each of which goes in exactly one mailbox, and there are n mailboxes, then each mailbox must get exactly one letter.

  Now let $f(x) = f(y) = b$. This means that x and y are in the same set of the partition of A. But this set is a singleton, so $x = y$.

Illustrating the lemma



f is not onto



f is onto

Using the lemma to prove uniqueness

- For each modulus m_j in the Chinese Remainder Theorem, $\mathbb{Z}_{m_j}$ has m_j elements. Therefore

  $$B = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

  has $M = m_1 \cdot \cdots \cdot m_k$ elements.

- So does $A = \mathbb{Z}_M$.

- Let $f : A \to B$ be the function

  $$f(x) = (x \bmod m_1, \ldots, x \bmod m_k).$$

  We claim that f is onto B. This is just a restatement of the existence part of the theorem: for any $(a_1, \ldots, a_k) \in B$, there is an x in $\mathbb{Z}_M$ such that

  $$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

  If x, y in $\mathbb{Z}_M$ are solutions to the congruences, we have $f(x) = f(y)$. By the lemma, $x = y$. Therefore there is at most one solution to the given congruences in $\mathbb{Z}_M$. (QED)