Fall 2013
Lecture 13: Modular inverses, induction

**announcements**

Reading assignment

**Induction**

- 5.1-5.2, 7th edition
- 4.1-4.2, 6th edition

---

**review: GCD**

\[
a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46,200
\]

\[
b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204,750
\]

\[
\text{GCD}(a, b) = 2^\min(3,1) \cdot 3^\min(1,2) \cdot 5^\min(2,3) \cdot 7^\min(1,1) \cdot 11^\min(1,0) \cdot 13^\min(0,1)
\]

**Factoring is expensive!**

Can we compute GCD(a, b) without factoring?

If \(a\) and \(b\) are positive integers, then

\[
\gcd(a, b) = \gcd(b, a \mod b)
\]

---

**review: euclid’s algorithm**

Repeatedly use the GCD fact to reduce numbers until you get GCD(x, 0) = x.

\[
\text{GCD}(660, 126) = \ ?
\]

\[
660 = 5 \cdot 126 + 30 \quad \text{GCD}(660, 126) = \text{GCD}(126, 30)
\]

\[
126 = 4 \cdot 30 + 6 \quad = \text{GCD}(30, 6)
\]

\[
30 = 5 \cdot 6 + 0 \quad = \text{GCD}(6, 0)
\]

\[
= 6
\]
bézout’s theorem

If \( a \) and \( b \) are positive integers, then there exist integers \( s \) and \( t \) such that
\[
\gcd(a, b) = sa + tb.
\]

extended euclid algorithm

- Can use Euclid’s Algorithm to find \( s \), \( t \) such that
  \[
  \gcd(a, b) = sa + tb
  \]
- e.g. \( \gcd(35,27) \):
  \[
  \begin{align*}
  35 &= 1 \cdot 27 + 8 \\
  27 &= 3 \cdot 8 + 3 \\
  8 &= 2 \cdot 3 + 2 \\
  3 &= 1 \cdot 2 + 1 \\
  2 &= 2 \cdot 1 + 0
  \end{align*}
  \]
- Substitute back from the bottom
  \[
  \begin{align*}
  1 &= 3 - 1 \cdot 2 \\
  &= 3 - 1 \cdot (8 - 2 \cdot 3) \\
  &= 3 - 1 \cdot (27 - 3 \cdot 8) \\
  &= 3 - 1 \cdot 27 + (-10) \cdot 8
  \end{align*}
  \]

multiplicative inverse \( \mod m \)

Suppose \( \gcd(a, m) = 1 \)

By Bézout’s Theorem, there exist integers \( s \) and \( t \) such that \( sa + tm = 1 \).

\( s \mod m \) is the multiplicative inverse of \( a \):
\[
1 = (sa + tm) \mod m = sa \mod m
\]

solving modular equations

Solving \( ax \equiv b \pmod{m} \) for unknown \( x \) when \( \gcd(a, m) = 1 \).

1. Find \( s \) such that \( sa + tm = 1 \)
2. Compute \( a^{-1} = s \mod m \), the multiplicative inverse of \( a \) modulo \( m \)
3. Set \( x = (a^{-1} \cdot b) \mod m \)
multiplicative cipher: \( f(x) = ax \mod m \)

For a multiplicative cipher to be invertible:
\[
f(x) = ax \mod m : \{0, ..., m-1\} \rightarrow \{0, ..., m-1\}
\]
must be one-to-one and onto

Lemma: If there is an integer \( b \) such that \( ab \mod m = 1 \), then the function \( f(x) = ax \mod m \) is one-to-one and onto.

mathematical induction

Method for proving statements about all integers \( n \geq 0 \).

– Part of sound logical inference that applies only in the domain of integers
    Not like scientific induction which is more like a guess from examples
– Particularly useful for reasoning about programs since the statement might be “after \( n \) times through this loop, property \( P(n) \) holds”

finding a pattern

- \( 2^0 - 1 = 1 - 1 = 0 = 3 \cdot 0 \)
- \( 2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1 \)
- \( 2^4 - 1 = 16 - 1 = 15 = 3 \cdot 5 \)
- \( 2^6 - 1 = 64 - 1 = 63 = 3 \cdot 21 \)
- \( 2^8 - 1 = 256 - 1 = 255 = 3 \cdot 85 \)
- ...

example

Solve: \( 7x \equiv 1 \pmod{26} \)
how do you prove it?

Want to prove $3 \mid 2^{2n} - 1$ for all integers $n \geq 0$

- $n = 0$
- $n = 1$
- $n = 2$
- $n = 3$
- $\ldots$

using the induction rule in a formal proof

1. Prove $P(0)$
2. Let $k$ be an arbitrary integer $\geq 0$
3. Assume that $P(k)$ is true
4. $\ldots$
5. Prove $P(k+1)$ is true
6. $P(k) \rightarrow P(k+1)$
7. $\forall k (P(k) \rightarrow P(k+1))$
8. $\forall n P(n)$

induction as a rule of Inference

Domain: integers $\geq 0$

$P(0)$

$\forall k (P(k) \rightarrow P(k + 1))$

$\therefore \forall n P(n)$

using the induction rule in a formal proof

1. Prove $P(0)$
2. Let $k$ be an arbitrary integer $\geq 0$
3. Assume that $P(k)$ is true
4. $\ldots$
5. Prove $P(k+1)$ is true
6. $P(k) \rightarrow P(k+1)$
7. $\forall k (P(k) \rightarrow P(k+1))$
8. $\forall n P(n)$

$\therefore \forall n P(n)$
5 steps to inductive proofs in English

**Proof:**
1. “By induction we will show that P(n) is true for every $n \geq 0$.”
2. “Base Case:” Prove P(0)
3. “Inductive Hypothesis:”
   
   Assume P(k) is true for some arbitrary integer $k \geq 0$.
4. “Inductive Step:” Want to prove that P(k+1) is true:
   
   Use the goal to figure out what you need.
   
   Make sure you are using I.H. and point out where you are using it. (Don’t assume P(k+1) !!!)
5. “Conclusion: Result follows by induction”

---

**induction example**

Want to prove $3 \mid 2^{2n} - 1$ for all $n \geq 0$.

---

**geometric sum**

$1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$ for all $n \geq 0$
$1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$ for all $n \geq 0$ 

**sum of first $n$ numbers**

For all $n \geq 1$: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

For all $n \geq 1$: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$