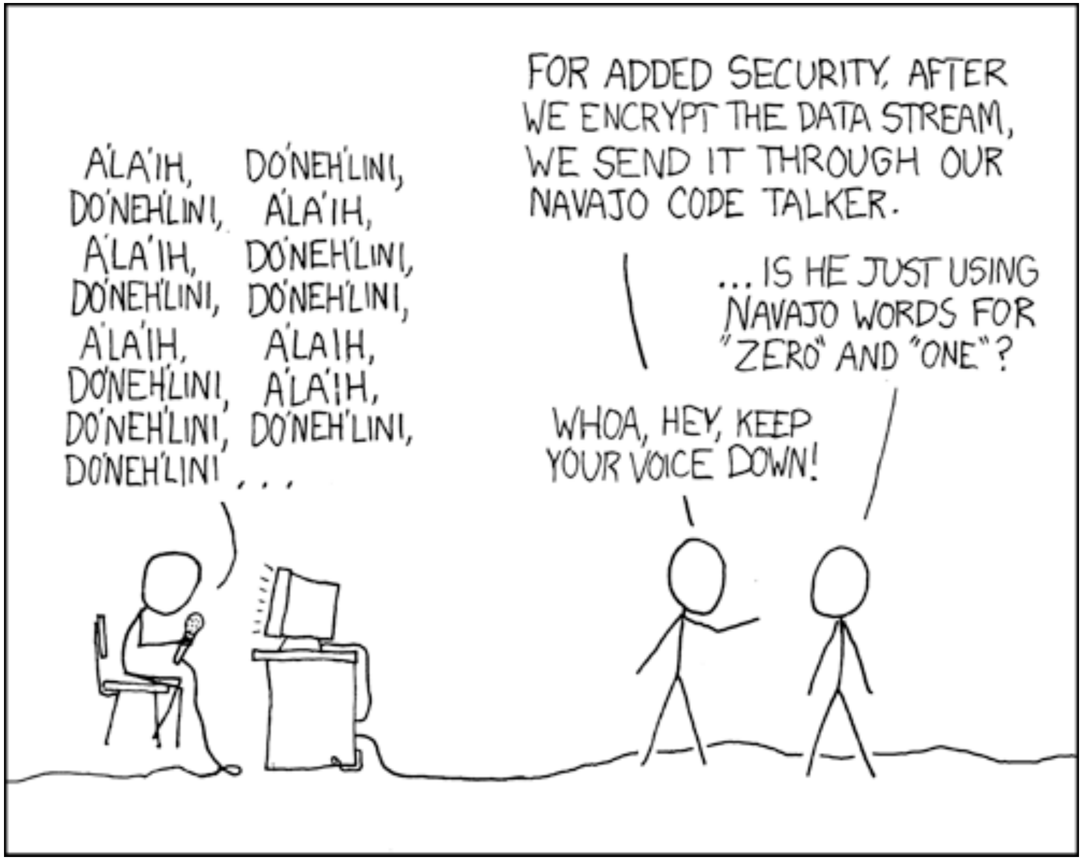
CSE 311

Foundations of Computing I

CSE 311: Foundations of Computing

Lecture 10: Modular Arithmetic



Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing

- Many significant applications
  - Cryptography
  - Hashing
  - Security

- Important tool set

Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

I'm ALIVE!

```
public class Test {
   final static int SEC_IN_YEAR = 364*24*60*60*100;
   public static void main(String args[]) {
      System.out.println(
         “I will be alive for at least ” +
         SEC_IN_YEAR * 101 + “ seconds.”
      );
   }
}
```

I’m ALIVE!

```
public class Test {
   final static int SEC_IN_YEAR = 364*24*60*60*100;
   public static void main(String args[]) {
      System.out.println(
         “I will be alive for at least ” +
         SEC_IN_YEAR * 101 + “ seconds.”
      );
   }
}
```

```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

 ----jGRASP: operation complete.
```

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists(k \in \mathbb{Z})\ \mathrm{b} = \mathrm{ka}$$

Check Your Understanding. Which of the following are true?

5 | 1	**25 | 5**	**5 | 5**	**3 |2**
1 | 5	**5 | 25**	**0 | 1**	**2 | 3**

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists(k \in \mathbb{Z})\ \mathrm{b} = \mathrm{ka}$$

Check Your Understanding. Which of the following are true?

5 | 1	**25 | 5**	**5 | 5**	**3 |2**
5 | 1 iff 1 = 5k	25 | 1 iff 1 = 25k	5 | 5 iff 5 = 5k	3 | 2 iff 2 = 3k
1 | 5	**5 | 25**	**0 | 1**	**2 | 3**
1 | 5 iff 5 = 1k	1 | 25 iff 25 = 1k	0 | 1 iff 1 = 0k	2 | 3 iff 3 = 2k

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:
Then, there exists *unique* integers *q*, *r* with $0 \leq r < d$ such that $a = dq + r$.

To put it another way, if we take a/d, we get a dividend and a remainder: *q* = *a* **div** *d* *r* = *a* **mod** *d*

Note: r ≥ 0 even if a < 0.
Not quite the same as `a % d`.

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:

Then, there exists *unique* integers *q*, *r* with $0 \le r < d$ such that $a = dq + r$.

To put it another way, if we take a/d, we get a dividend and a remainder: $q = a$ **div** d $\qquad$ $r = a$ **mod** d

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

```
 ----jGRASP exec: java Test2
-1

 ----jGRASP: operation complete.
```

Note: r ≥ 0 even if a < 0.
Not quite the same as **`a % d`.**

Arithmetic, mod 7

$$a +_7 b = (a + b) \bmod 7$$

$$a \times_7 b = (a \times b) \bmod 7$$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a \in \mathbb{Z}, b \in \mathbb{Z}, \mathrm{m} \in \mathbb{Z}$:

$$a \equiv_m b \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

$A \equiv_2 0$

$1 \equiv_4 0$

$A \equiv_{17} -1$

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a \in \mathbb{Z}, b \in \mathbb{Z}, \mathrm{m} \in \mathbb{Z}$:

$$a \equiv_m b \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

$A \equiv_2 0$

This statement is the same as saying "A is even"; so, any A that is even (including negative even numbers) will work.

$1 \equiv_4 0$

This statement is false. If we take it mod 1 instead, then the statement is true.

$A \equiv_{17} -1$

If A = 17x – 1 = 17x + 16, then it works.

Note that (m – 1) mod m = ((m mod m) + (-1 mod m)) mod m
= (0 + -1) mod m = -1 mod m

Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. Then, $a \equiv_m b$ if and only if a mod m = b mod m.

Suppose that $a \equiv_m b$.

Suppose that a mod m = b mod m.

Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. Then, $a \equiv_m b$ if and only if a mod m = b mod m.

Suppose that $a \equiv_m b$.

Then, m | (a – b) by definition of congruence.

So, a – b = km for some integer k by definition of divides.

Therefore, a = b+km.

Taking both sides modulo m we get:

a mod m=(b+km) mod m = b mod m.

Suppose that a mod m = b mod m.

By the division theorem, a = mq + (a mod m) and

b = ms + (b mod m) for some integers q,s.

Then, a – b = (mq + (a mod m)) – (mr + (b mod m))

= m(q – r) + (a mod m – b mod m)

= m(q – r) since a mod m = b mod m

Therefore, m | (a-b) and so $a \equiv_m b$.

Modular Arithmetic: Another Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $\mathbf{a + c \equiv_m b + d}$

Modular Arithmetic: Another Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $\mathbf{a + c \equiv_m b + d}$

Suppose $a \equiv_m b$ and $c \equiv_m d$. Unrolling definitions gives us some k such that $a – b = km$, and some j such that $c – d = jm$.

Adding the equations together gives us $(a + c) – (b + d) = m(k + j)$. Now, re-applying the definition of mod gives us $a + c \equiv_m b + d$.

Modular Arithmetic: Another-nother Property

Let m be a positive integer.
If $a \equiv_m b$ and $c \equiv d$, then **$ac \equiv_m bd$**

Modular Arithmetic: Another-nother Property

Let m be a positive integer.
If $a \equiv_m b$ and $c \equiv_m d$, then **$ac \equiv_m bd$**

Suppose $a \equiv_m b$ and $c \equiv_m d$. Unrolling definitions gives us some k such that $a - b = km$, and some j such that $c - d = jm$.

Then, $a = km + b$ and $c = jm + d$. Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + jmb + bd$.

Re-arranging gives us $ac - bd = m(kjm + kd + jb)$. Using the definition of mod gives us $ac \equiv_m bd$.

Example

Let n be an integer.
Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

Example

Let n be an integer.
Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

Let's start by looking a a small example:

$0^2 = 0 \equiv_4 0$

$1^2 = 1 \equiv_4 1$

$2^2 = 4 \equiv_4 0$

$3^2 = 9 \equiv_4 1$

$4^2 = 16 \equiv_4 0$

Example

Let n be an integer.
Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

Let's start by looking a a small example:

$0^2 = 0 \equiv_4 0$

$1^2 = 1 \equiv_4 1$

$2^2 = 4 \equiv_4 0$

$3^2 = 9 \equiv_4 1$

$4^2 = 16 \equiv_4 0$

It looks like

$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and

$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Example

Let n be an integer.
Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

Case 1 (n is even):

Case 2 (n is odd):

Example

Let n be an integer.
Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

Let's start by looking a a small example:

$0^2 = 0 \equiv_4 0$
$1^2 = 1 \equiv_4 1$
$2^2 = 4 \equiv_4 0$
$3^2 = 9 \equiv_4 1$
$4^2 = 16 \equiv_4 0$

It looks like
$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and
$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Case 1 (n is even):
Suppose $n \equiv_2 0$.
Then, $n = 2k$ for some k.
So, $n^2 = (2k)^2 = 4k^2$. So, by definition of congruence, $n^2 \equiv_4 0$.

Case 2 (n is odd):
Suppose $n \equiv_2 1$.
Then, $n = 2k + 1$ for some k.
So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. So, by definition of congruence, $n^2 \equiv_4 1$.