CSE 311

Foundations of Computing I

* All slides are a combined effort between previous instructors of the course

Modular Arithmetic

Definition: "a is congruent to b modulo m"

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

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

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

A ≡ 0 (mod 2)

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

1 ≡ 0 (mod 4)

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

A ≡ -1 (mod 17)

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

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*

```
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

This Course So Far

Framework for Reasoning:

Logic → More Logic → More More Logic → Proofs

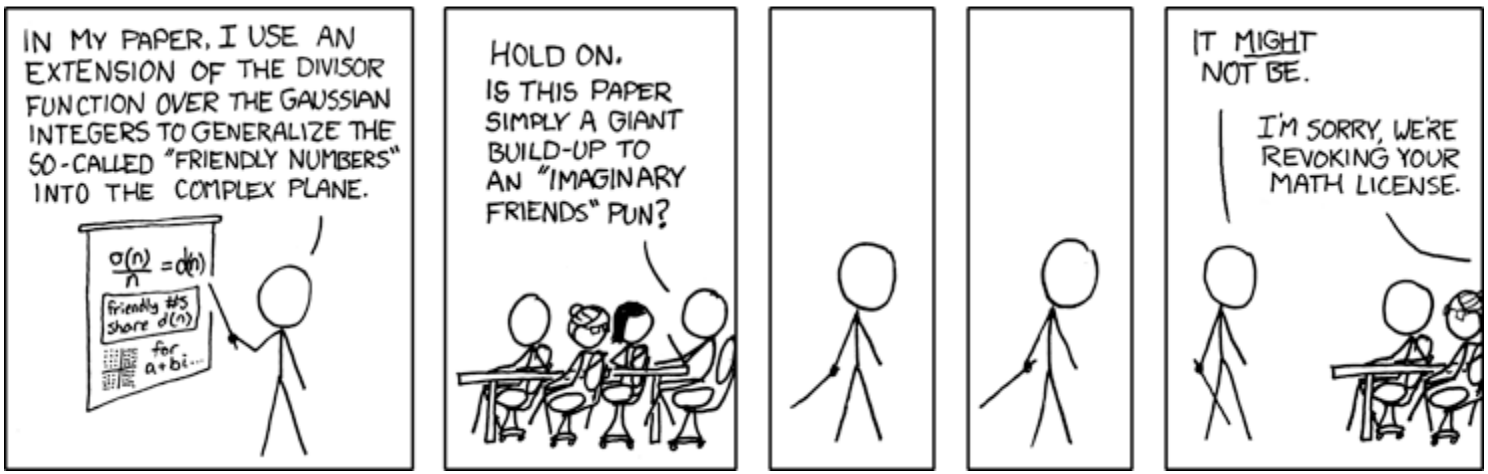
Things to Reason About

Number Theory

Sets (more more more logic…?)

CSE 311: Foundations of Computing

Lecture 11: Modular Arithmetic and Applications



Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer.
Then, $a \equiv b \pmod{m}$ if and only if a mod m = b mod m.

Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ 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:

$$a \bmod m=(b+km) \bmod m = b \bmod m.$$

Suppose that a mod m = b mod m.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (mr + (b \bmod m))$
$= m(q - r) + (a \bmod m - b \bmod m)$
$= m(q - r)$ since a mod m = b mod m

Therefore, $m \mid (a-b)$ and so $a \equiv b \pmod{m}$.

Modular Arithmetic: Another Property

Let m be a positive integer. If a ≡ b (mod m) and c ≡ d (mod m), then **a + c ≡ b + d (mod m)**

Suppose a ≡ b (mod m) and c ≡ d (mod m). 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 congruence gives us a + c ≡ b + d (mod m).

Modular Arithmetic: Another-nother Property

Let m be a positive integer. If a ≡ b (mod m) and c ≡ d (mod m), then **ac ≡ bd (mod m)**

Suppose a ≡ b (mod m) and c ≡ d (mod m). 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 congruence gives us ac ≡ bd (mod m).

Example

Let n be an integer.
Prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like
$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

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

Case 2 (n is odd):
Suppose $n \equiv 1 \pmod 2$.
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, $n^2 \equiv 1 \pmod 4$.

n-bit Unsigned Integer Representation

- Represent integer x as sum of powers of 2:

  If $x = \sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0,1\}$

  then representation is $b_{n-1}...b_2\ b_1\ b_0$

99 = 64 + 32 + 2 + 1

18 = 16 + 2

- For n = 8:

  99: 0110 0011

  18: 0001 0010

Sign-Magnitude Integer Representation

n-bit signed integers

Suppose $-2^{n-1} < x < 2^{n-1}$

First bit as the sign, n-1 bits for the value

99 = 64 + 32 + 2 + 1

18 = 16 + 2

For n = 8:

99: 0110 0011

-18: 1001 0010

Any problems with this representation?

Two's Complement Representation

n bit signed integers, first bit will still be the sign bit

Suppose $0 \leq x < 2^{n-1}$,
 x is represented by the binary representation of x

Suppose $0 \leq x \leq 2^{n-1}$,
 $-x$ is represented by the binary representation of $2^n - x$

Key property: Twos complement representation of any number y is equivalent to y mod 2^n so arithmetic works mod 2^n

99 = 64 + 32 + 2 + 1
18 = 16 + 2

For n = 8:
 99: 0110 0011
 -18: 1110 1110

Sign-Magnitude vs. Two's Complement

-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1111	1110	1101	1100	1011	1010	1001	0000	0001	0010	0011	0100	0101	0110	0111

Sign-bit

-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111

Two's complement