CS70 Fall 2013
Discrete Math and Probability Theory

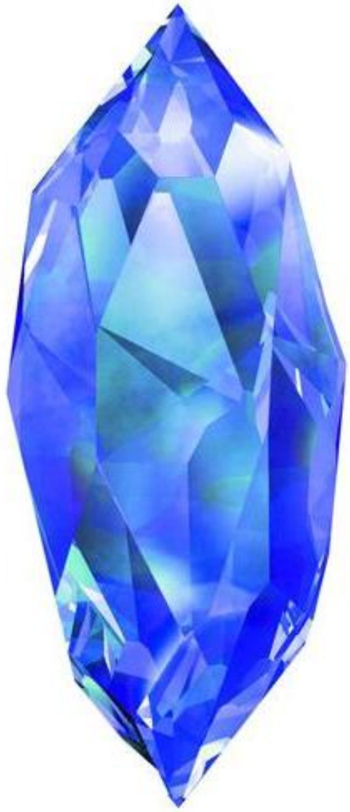
Umesh V. Vazirani

U.C. Berkeley

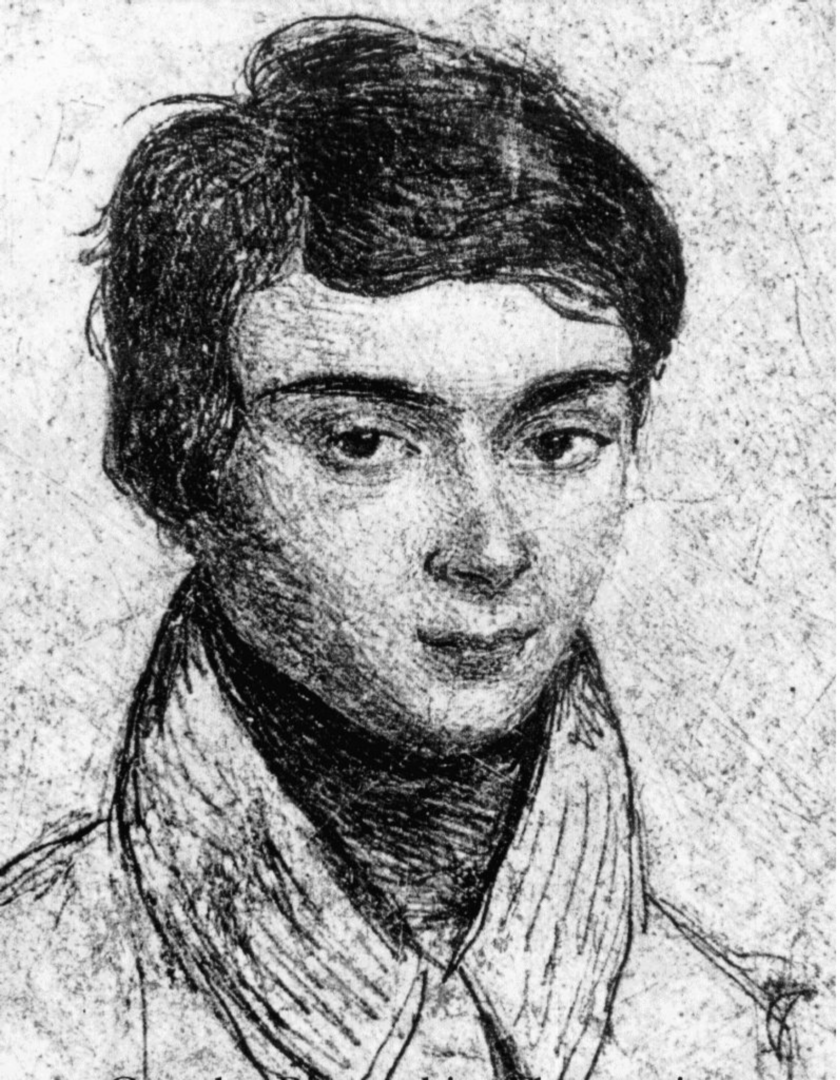
Lecture 6: Modular Arithmetic

Modular Arithmetic

1. Mathematical crystals: highly symmetric mathematical objects



Reliable storage and communication
Security and cryptography
…



Évariste Galois (1811 – 1832)

- 1828: Failed entrance exam for École Polytechnique
- Spent 9 months in prison for what was interpreted as a threat against king's life.
- Fatally wounded in a duel over a woman.
- Spent his last night outlining his mathematical ideas in three attached manuscripts.
- Laid foundations of group theory.

$a \quad , \quad m$

Arithmetic mod m

$a = m q + r$

Divide a by m

Remainder r

$\{0, 1, \dots, m-1\}$

Time : mod 12

Days of Week:

Sunday = 0

Monday = 1

⋮

Saturday = 6

$5 = 2 + 10 \pmod 7$

$3 = 2 + 365 \pmod 7$

$2 + 365 \times 50 \pmod 7$

$= 2 + 1 \times 1 \pmod 7$

$= 3$

Arithmetic mod m

$+ \;,\; \times \;,\; -$

Two ways: (I) arithmetic first
Then reduce (mod m)

$\boxed{\text{(II) Reduce (mod m) whenever you feel like it.}}$

$6 \equiv -15 \pmod 7$

$-15 \pmod 7$

$-15 = 7 \times (-3) + 6$

$$[x + 25 \equiv 3] \pmod 7$$

$$x \equiv 3 - \overset{4}{25} \pmod 7$$

$$\equiv -22 \pmod 7$$

$$\equiv -1 \pmod 7$$

$$\equiv 6$$

$$-1 = 7 \times -1 + 6$$

⋮	⋮	⋮	⋮	⋮
35	36		38	34
28	29		31	27
21	$\boxed{22}$	$\boxed{23}$	24	$\boxed{20}$
14	15	16	17	13
7	8	9	$\boxed{10}$	6
0	1	2	3	−1
−7	−6	$\boxed{-5}$	$\boxed{-4}$	−8
−14	$\boxed{-13}$	−12	−11	−15
−21	−20	−19	−18	−22
−28	−27	−26	−25	⋮
⋮	⋮	⋮	⋮	
Sunday	Monday	Tue	2 − 1 = 1	1 + 2 = 3 3 − 2 = 1

54

$a \quad (\mathrm{mod}\ m)$ $\quad$ $\underline{\underline{r}} = a\ (\mathrm{mod}\ m)$

$a = mq + r$ $\quad$ $r \in \{0, 1, \ldots, m-1\}$

$a - r = \underline{\underline{m}}q$

$a \equiv b\ (\mathrm{mod}\ m)$ iff $a - b$ div by m.

$a - b = mq$

$r = a\ (\mathrm{mod}\ m)$

$r \equiv a\ (\mathrm{mod}\ m)$

Thm $a \equiv b \pmod{m}$ $\quad c \equiv d \pmod{m}$

then $a + c \equiv b + d \pmod{m}$ and

$$a \cdot c \equiv b \cdot d \pmod{m}$$

$$a = b + qm \qquad c = d + q'm$$

$$\begin{aligned} a \cdot c &= (b + qm)(d + q'm) \\ &= bd + bq'm + dqm + qq'm^2 \\ &= bd + m\underbrace{[bq' + dq + qq'm]}_{} \end{aligned}$$

$$ac \equiv bd \pmod{m}$$

Definition

8 bits 256

-128 to +127

Property

Two's complement representation allows the use of binary arithmetic operations on signed integers, yielding the correct 2's complement results.

Positive Numbers

Positive 2's complement numbers are represented as the simple binary.

Negative Numbers

Negative 2's complement numbers are represented as the binary number that when added to a positive number of the same magnitude equals zero.

Calculation of 2's Complement

To calculate the 2's complement of an integer, invert the binary equivalent of the number by changing all of the ones to zeroes and all of the zeroes to ones (also called 1's complement), and then add one.

For example,

$\texttt{0001 0001}_{\text{(binary 17)}} \Rightarrow \texttt{1110 1111}_{\text{(two's complement -17)}}$

`NOT(0001 0001) = 1110 1110 (Invert bits)`

Two's complement

Modular arithmetic is nicely illustrated in *two's complement*, the most common format for storing signed integers. It uses n bits to represent numbers in the range $[-2^{n-1}, 2^{n-1}-1]$ and is usually described as follows:

- Positive integers, in the range 0 to $2^{n-1}-1$, are stored in regular binary and have a leading bit of 0.
- Negative integers $-x$, with $1 \le x \le 2^{n-1}$, are stored by first constructing x in binary, then flipping all the bits, and finally adding 1. The leading bit in this case is 1.

(And the usual description of addition and multiplication in this format is even more arcane!)

$[-2^{n-1}, 2^{n-1}-1]$ $\qquad$ $[-128, 127]$

To represent x write $x \bmod 2^n$.

$x \pmod{256}$

Arithmetic mod m:

$+, -, \times \pmod{m}$

$\div$ $\qquad \mathbb{R} \qquad \div z$, $z \neq 0$, same as $\times \frac{1}{z}$

$$z \times \frac{1}{z} = 1$$

$$\frac{4}{5} \pmod{7}$$

$$= 4 \times 3 \pmod{7}$$

$$= 5$$

$$1 = 5 \times 3 \pmod{7}$$

$$3 = \frac{1}{5} \pmod{7}$$

$$5 = \frac{4}{5} \pmod{7}$$

$$5 \times 5 = 4 \pmod{7}$$

$\frac{1}{5} \pmod 7$

$1 \equiv 8 \equiv 15 \equiv 22 \equiv 29 \equiv 36 \ldots$

$\frac{1}{5} \equiv \frac{15}{5} \equiv 3 \pmod 7$

$\frac{1}{2} \pmod{12}$

$1 \equiv 13 \equiv 25 \equiv 37 \equiv 49 \equiv 61$

$1 + 12 \cdot q$

$\frac{1}{a} \pmod m$

Case 1 a, m have no common divisors
Possible

Case 2 : a, m have a common divisor.
Impossible.

$\frac{1}{a} \pmod m = a^{-1} \pmod m$ exists

iff $\boxed{\gcd(a,m) = 1}$.

$\gcd(a,b) = d$

d divides a

" b

$d | a$ & $d | b$.

If $d' | a$ & $d' | b \Rightarrow d' | d$.

$\gcd(30, 42) = 6$

$30 = 2 \times 3 \times 5$

$42 = 2 \times 3 \times 7$

Euclid's Algorithm: ~300 BC.
Gabriel Lame 1844

$a = 42 \qquad b = 30.$

$\gcd(\underline{\underline{a}}, \underline{\underline{b}})$

$42 = \underline{\underline{30}} \times 1 + \underline{\underline{12}}$

$a = bq + r \qquad 0 \le r < b$

$\gcd(a,b) = \gcd(b,r)$

$d \mid a \quad \& \quad d \mid b \Rightarrow d \mid a - bq$

$a = dz \qquad b = dz'$

$a - bq = dz - dz'q$
$= d[z - z'q]$

$$42 = \underline{\underline{30}} \times 1 + \underline{\underline{12}}$$

$$30 = \underline{\underline{12}} \times 2 + \underline{\underline{6}}$$

$$12 = \underline{\underline{6}} \times 2 + \underline{\underline{0}}.$$

$$\gcd(42, 30)$$
$$= \gcd(30, 12)$$
$$= \gcd(12, 6)$$
$$= 6$$

```
algorithm gcd(x,y)
  if y = 0 then return(x)
  else return(gcd(y,x mod y))
```

$x \geq y$.

$x = yq + r$

$\text{x mod y} = r$.

Bezout's Identity or Extended Euclid:

$$\gcd(a,b) = d.$$

$$\exists\, x, y: \quad a\underline{\underline{x}} + b\underline{\underline{y}} = d$$

Div by $a \pmod m$ $\qquad a^{-1} \equiv \frac{1}{a} \pmod m$

$$\gcd(a,m) = 1.$$

$$x, y: \quad ax + my = 1.$$

$$a\underline{\underline{x}} \equiv 1 \pmod m$$