

Number Theory I:

Extended Euclidean Algorithm

02/17 Prof. Forrest

Warm-up

1. Discuss with your neighbors whether desserts can be savory (i.e. must they be sweet)

2. Give the Lagrange basis polynomials (e.g. $\{l_0(x), l_1(x), l_2(x), l_3(x)\}$) for the following shares: $f(1)=3, f(2)=6, f(3)=1, f(4)=2$
or points

$$l_0(x) = \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} \cdot \frac{x-4}{1-4} \leftarrow$$

$$l_0(1) = 1 \quad f(3) = 0$$

Logistics

- Codelet 2 has been cracked
everyone did fine.

Real Shamir's Secret Sharing

Secret

$$f(x) = \text{Secret} + \sum_{i=1}^{k-1} a_i x^i \quad \text{where } a_i \in \text{Domain}_{\text{random}}$$

$(1, f(1))$ $(2, f(2))$ $(3, f(3))$ $(k, f(k))$ $(n, f(n))$

distribute n
shares $n \geq k$

k people are need to reconstruct the secret
and no group of people $< k$ learn anything
about the secret.

Challenge: (1) integer overflow (e.g., what if coefficients are large)
(2) precision (e.g., $2/3$)

$$x, y \in \mathbb{R}$$

1.2

1.3333...

$$x \cdot y = 1$$

$\hat{=}$ multiplicative inverse of x

$$x \cdot x^{-1} = 1$$

$\equiv$

$$x \cdot \frac{1}{x} = 1$$

$$x = 3 \quad x^{-1} = 1/3$$

$$1 = 2 x^{-1}, \quad x^{-1} \in \mathbb{Z}$$

Division

$$\frac{x}{y}$$

$\equiv$

$$x y^{-1}$$



$$x^{-1} \in \mathbb{Z}$$

$$1/2$$

Division Theorem

For integers $d > 0$ and n ,
the quantity $\underline{n \bmod d}$ is the
unique integer r and q when
 $0 \leq r < d$ and $dq + r = n$

$$n \bmod d = r \quad q := \left\lfloor \frac{n}{d} \right\rfloor$$

$\uparrow$
remainder

$$n = \left\lfloor \frac{n}{d} \right\rfloor \cdot d + (n \bmod d)$$

$\uparrow$ quotient $\uparrow$ divisor $\uparrow$ remainder

$$(1) \quad n = 7 \quad d = 3 \quad 7 = 7 \bmod 3 + \text{---}$$

$r = 1 \quad q = 2$
 $7 = 2 \cdot 3 + r$

$$-21 \bmod 10$$

$$-21 = 4 \cdot 10 + \checkmark$$

$\downarrow$
 $-3 \quad 4$

properties mod. arithmetic

$$n \bmod n = 0$$

$$(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$$

$$a \cdot b \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$$

$$2 \cdot 5 \bmod 6 = 4$$

$$\begin{array}{r} 2 \bmod 6 \\ \hline 2 \end{array}, \begin{array}{r} 5 \bmod 6 \\ \hline 5 \end{array} = 10 \bmod 6 = 4$$

$$a \cdot b \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$$

$p \rightarrow q$

$$a = cn + r$$

$$r = a \bmod n$$

$$b = dn + s$$

$$s = b \bmod n$$

$$a \cdot b \bmod n =$$

$$= ((cn + r) \cdot (dn + s)) \bmod n$$

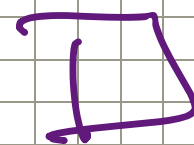
$$= (c d n^2 + c n s + d n r + r s) \bmod n$$

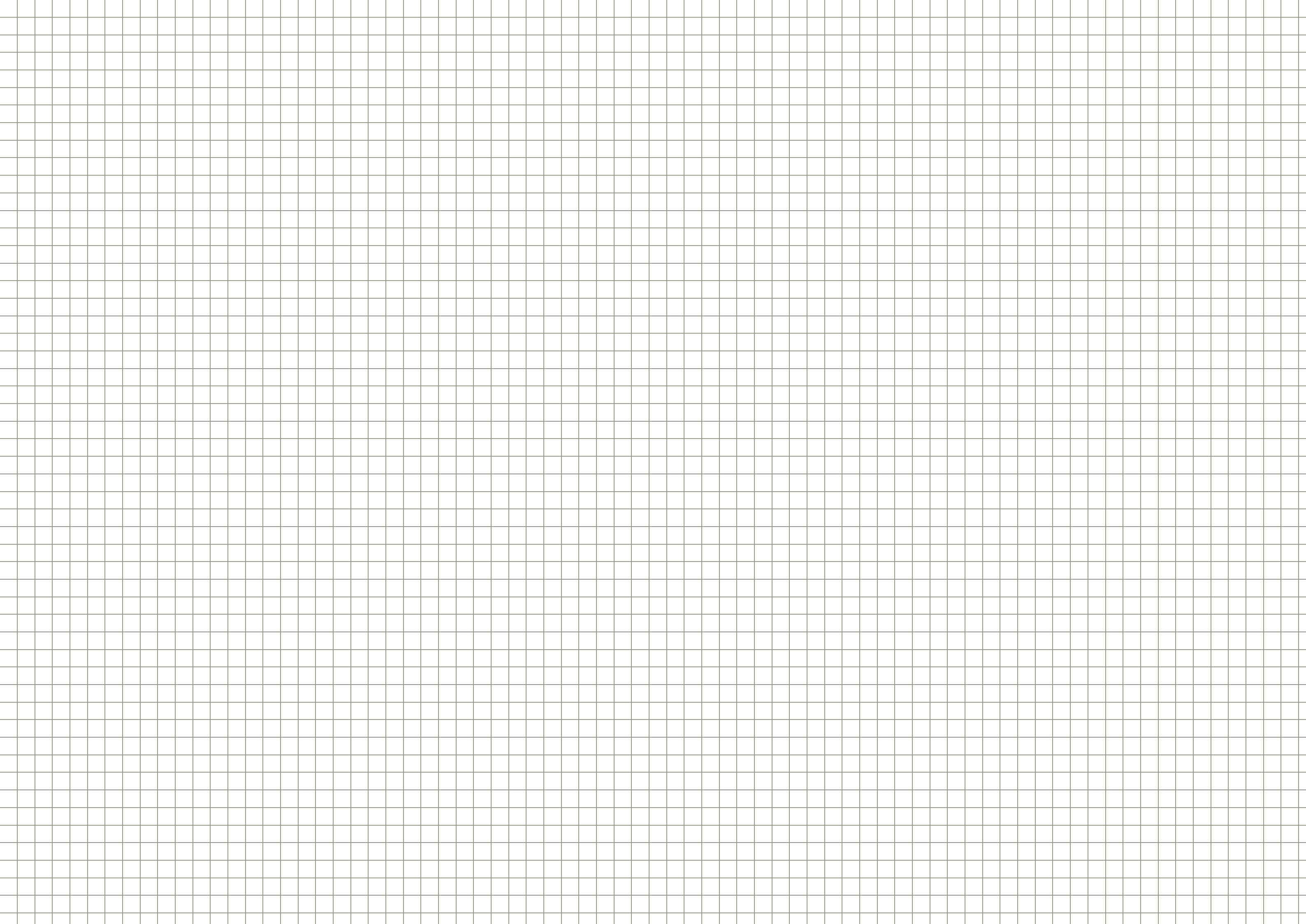
$$= ((c d n + c s + d r) n + r s) \bmod n$$

$$= \cancel{(c d n + c s + d r) n} \bmod n + r s \bmod n$$

$$= r s \bmod n$$

$$= (a \bmod n) \cdot (b \bmod n) \bmod n$$





Definition: Divisibility

for two integers $m > 0$ and n we write

$m \mid n$ to denote the proposition that

$n \bmod m = 0$. If $m \mid n$, then we

say that m divides n (or that m evenly divides n), that n is a multiple of m , and that m is a factor of n .

$$a \mid 0$$

$$1 \mid a$$

are these true?
for some positive
integer a

$$0 \bmod a = 0$$

$$a \bmod 1 = 0$$

$$r = 6 \bmod 1$$

$$1 \cdot q + r = 6$$

def Greatest Common Divisor
GCD

The greatest common divisor of two
positive integers n, m ($\gcd(n, m)$)
is the largest $d \in \mathbb{Z}^{>0}$ s.t.
 $d|n$ and $d|m$

$$\gcd(6, 27) = 3$$

$$\gcd(12, 18) = 6$$

$$\gcd(1, 9) = 1$$

Euclid(n, m)

Input: $n, m \in \mathbb{Z}^{>0}$ and $m \geq n$

Output: $\text{gcd}(n, m)$

1. if $m \bmod n = 0$ then

2. return n

3. else

4. return Euclid($m \bmod n, n$)

Euclid(17, 42)

Bézout's Identity:

Let n, m be any positive integers, and let $g = \gcd(n, m)$ be r , then there exists

$$x, y \in \mathbb{Z} \text{ such that } xn + ym = r$$

$$2, 9$$

$$\gcd(2, 9) = 1$$

$$1 = x(2) + y(9) \quad \text{mod } 9$$

$$1 = 5 - 2 + (-1)(9)$$

$$= 10 + (-9)$$

$$= 1$$

$$\cancel{\gcd(2, 9)}^1 = (x \cdot 2 + \cancel{y \cdot 9})^0 \pmod 9$$

$$1 = x \cdot 2 \pmod 9$$

x is inverse of 2 on $\mathbb{Z}_9$

$\{0, 1, 2, 3, \dots, 8\}$

$$x = 5$$

Extended Euclidean Algorithm (n, m)

Input: $n, m \in \mathbb{Z}^{>0}$ and $m \geq n$

Output: $x, y, r \in \mathbb{Z}$ where $\gcd(n, m) = r = xn + ym$

1. if $m \bmod n = 0$ then

2. return $1, 0, n$ $// (1) \cdot n + (0) \cdot m = n = \gcd(n, m)$
as $n \mid m$

3. else:

4. $x, y, r = \text{extended Euclidean Algorithm}(m \bmod n, n)$

5. return $y - \lfloor \frac{m}{n} \rfloor \cdot x, x, r$

if p is prime then
every nonzero $a \in \mathbb{Z}_p$ has
a multiplicative inverse

- pick up next class w/
proof of Euler's and
a better trace of the
algo.