Week 5

Saturday, March 23, 2024 3:02 PM

5.1

$a = dq + r \rightarrow$ a: dividend, d: divisor, q: quotient, r: remainder

$q = a \text{ div } d$ $\quad r = a \bmod d$

$a \equiv b \pmod M$ iff M divides $(a-b)$ / $(a-b)$ is divisible by M

- $17 \equiv 5 \pmod 6$
- $24 \not\equiv 14 \pmod 6$

Modular Arithmetic:

if $a \equiv b \pmod M$ and $c \equiv d \pmod M$:

- $a+c \equiv b+d \pmod M$
- $ac \equiv bd \pmod M$

- $(a+b) \pmod M = ((a \bmod M) + (b \bmod M)) \bmod M$
- $(ab) \pmod M = ((a \bmod M) \cdot (b \bmod M)) \bmod M$

Modular exponentiation:

- convert exponent to binary, multiply from there
- example: compute $572^{29} \bmod 713$:

$29 = 16+8+4+1$

$572^{29} = 572^{16} \cdot 572^8 \cdot 572^4 \cdot 572$

$572^2 \bmod 713 = 327184 \bmod 713 = 630$

$572^4 \bmod 713 = (572^2 \bmod 713)^2 \bmod 713 = 630^2 \bmod 713 = 472$

$572^8 \bmod 713 = (572^4 \bmod 713)^2 \bmod 713 = 328$

$572^{16} \bmod 713 = (572^8 \bmod 713)^2 \bmod 713 = 634$

$(634 \times 328 \times 472 \times 630) \bmod 713 = 113$

5.2

- Infinitely many primes ← Euclid's Theorem
- n is prime if no prime $p \leq \sqrt{n}$ divides n
- Euclidean algorithm:

```
procedure gcd(a, b):
    x := a
    y := b
    while y > 0:
        r := x mod y
        x := y
        y := r
    return x
```

- Let $a = bq + r$. Then, $\gcd(a, b) = \gcd(b, r)$