Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

Imdad ullah Khan

Prime Numbers

Definition

A positive integer p is prime if it has exactly two divisors, namely 1 and p

1 is not prime

Definition

A positive integer n is composite if it has a divisor d, $1 < d < n$

1 is not composite

Greatest common divisor

$\text{GCD}(a, b) :=$ the greatest common divisor

$\triangleright$ the largest integer d that divides both a and b

$\text{GCD}(24, 32) = 8$

$\text{GCD}(22, 24) = 2$

$\text{GCD}(15, 5) = 5$

$\text{GCD}(25, 15) = 5$

$\text{GCD}(13, 20) = 1$

$\text{GCD}(11, 33) = 11$

Lemma: p is prime $\implies \forall\, a \in \mathbb{Z}\;\; \text{GCD}(p, a) = 1$ or p

$\triangleright \because$ p has only two divisors 1 and p

Greatest common divisor

$\text{GCD}(a, b) :=$ the greatest common divisor

$\triangleright$ the largest integer d that divides both a and b

a and b are **relatively prime** if $\text{GCD}(a, b) = 1$

Equivalently, a and b have no common factors

$\text{GCD}(25, 16) = 1, \quad \text{GCD}(24, 25) = 1$

A prime number p is relatively prime to all integers except its multiples

Greatest common divisor

$\text{GCD}(a, b) :=$ the greatest common divisor

$\triangleright$ the largest integer d that divides both a and b

We can find $\text{GCD}(a, b)$ by

finding all divisors of a and b, then

find the common divisors, and then

find the greatest among the commons

Greatest common divisor

$\textsc{gcd}(a, b) :=$ the greatest common divisor

$\triangleright$ the largest integer d that divides both a and b

We can find $\textsc{gcd}(a, b)$ from the prime factorization of a and b

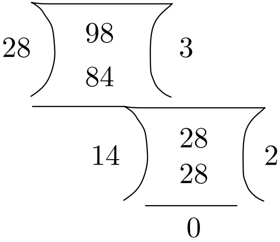
$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

$$\textsc{gcd}(a, b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \dots p_n^{\min\{a_n,b_n\}}$$

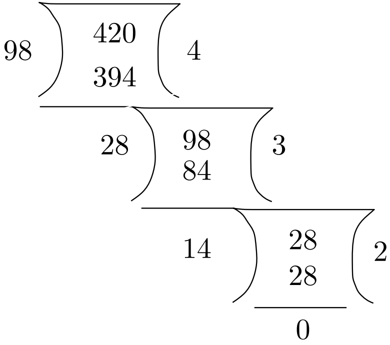
$$\begin{aligned} 98 &= 2 \cdot 7 \cdot 7 && = 2^1\, 3^0\, 5^0\, 7^2\, 11^0 \dots \\ 420 &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 && = 2^2\, 3^1\, 5^1\, 7^1\, 11^0 \dots \\ \textsc{gcd}(98, 420) &= && = 2^1\, 3^0\, 5^0\, 7^1\, 11^0 \dots = 14 \end{aligned}$$

GCD: Euclidean Algorithm

GCD$(28, 98)$

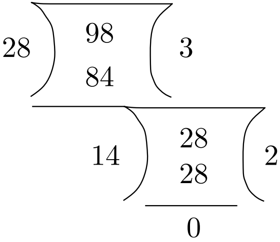


GCD$(98, 420)$

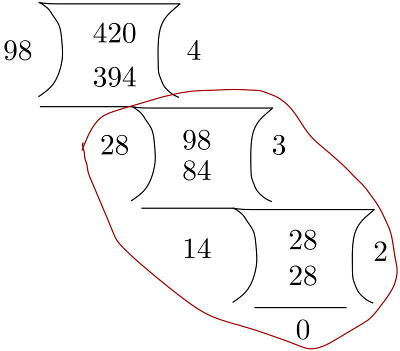


GCD: Euclidean Algorithm

GCD$(28, 98)$



GCD$(98, 420)$



Theorem (Euclid)

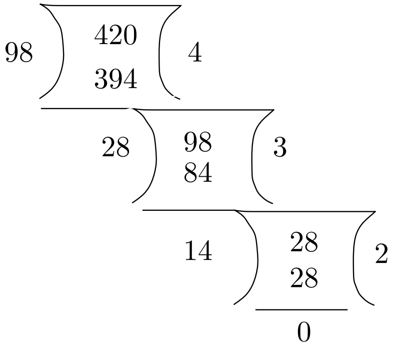
If $a = qb + r$, *then* GCD(a, b) $=$ GCD(b, r)

GCD: Euclidean Algorithm

Theorem (Euclid)

If $a = qb + r$, then $\text{GCD}(a, b) = \text{GCD}(b, r)$

$\text{GCD}(98, 420)$



$a = 420,\ b = 98$

$\triangleright\ 420 = 98 \cdot 3 + 28$

$\text{GCD}(420, 98) = \text{GCD}(98, 28)$

$\triangleright\ 98 = 28 \cdot 2 + 14$

$\text{GCD}(98, 28) = \text{GCD}(28, 14)$

$\triangleright\ 28 = 14 \cdot 2 + 0$

$\text{GCD}(28, 14) = \text{GCD}(14, 0) = 14$

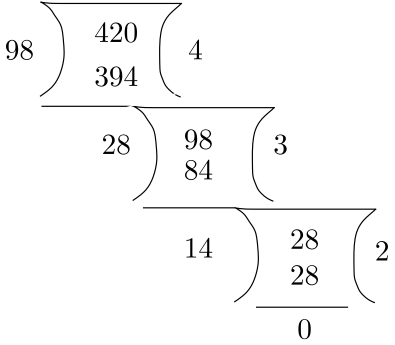
$\text{GCD}(420, 98) = 14$

GCD: Euclidean Algorithm

Theorem (Euclid)

If $a = qb + r$, *then* $\text{GCD}(a, b) = \text{GCD}(b, r)$

$\text{GCD}(98, 420)$



Algorithm GCD Computation

function $\text{GCD}(a, b)$
  if $b = 0$ **then**
    return a
  else
    $r \leftarrow a \% b$
    return $\text{GCD}(b, r)$

GCD: Euclidean Algorithm

Theorem (Euclid)

If $a = qb + r$, *then* $\text{GCD}(a, b) = \text{GCD}(b, r)$

Proof: **Case 1:** $r = 0 \implies \text{GCD}(b, r) = \text{GCD}(b, 0) = b$, as $b \mid 0$

$r = 0 \implies a = qb$, so $\text{GCD}(a, b) = b = \text{GCD}(b, r)$

Case 2: $r > 0$

Let d be a common divisor of b and r $\quad b = xd$ and $r = yd$

$a = qb + r = (qx)d + yd = (qx + y)d \implies d \mid a$

Let d be a common divisor of a and b $\quad a = sd$ and $b = td$

$r = a - qb = sd - (qt)d = (s + qt)d \implies d \mid r$

So d is a common divisor of $a, b \leftrightarrow d$ is a common divisor of b, r

GCD: Extended Euclidean Algorithm

Theorem

For all a, b, $\exists\, s, t: \quad sa + tb = \textsc{gcd}(a, b)$

$a = 420, \; b = 98$

$\triangleright\; 420 = 98 \cdot 3 + 28$

$\textsc{gcd}(420, 98) = \textsc{gcd}(98, 28)$

$\triangleright\; 98 = 28 \cdot 2 + 14$

$\textsc{gcd}(98, 28) = \textsc{gcd}(28, 14)$

$\triangleright\; 28 = 14 \cdot 2 + 0$

$\textsc{gcd}(28, 14) = \textsc{gcd}(14, 0) = 14$

$\textsc{gcd}(420, 98) = 14$

$\textsc{gcd}(420, 98) = 14$

$\triangleright\; 14 = 98 - 3 \cdot 28$

$\textsc{gcd}(420, 98) = 98 - 3 \cdot 28$

$\triangleright\; 28 = 420 - 98 \cdot 4$

$\textsc{gcd}(420, 98) = 98 - 3(420 - 4 \cdot 98)$

$\textsc{gcd}(420, 98) = -3 \cdot 420 + 13 \cdot 98$

$s = -3, \quad t = 13$

GCD: Extended Euclidean Algorithm

Theorem

For all a, b, $\exists\, s, t : \; sa + tb = \textsc{gcd}(a, b)$

$a = 899, \;\; b = 493$

$\triangleright \; 899 = 1 \cdot 493 + 406$

$\textsc{gcd}(899, 493) = \textsc{gcd}(493, 406)$

$\triangleright \; 493 = 1 \cdot 406 + 87$

$\textsc{gcd}(493, 406) = \textsc{gcd}(406, 87)$

$\triangleright \; 406 = 4 \cdot 87 + 58$

$\textsc{gcd}(406, 87) = \textsc{gcd}(87, 58)$

$\triangleright \; 87 = 1 \cdot 58 + 29$

$\textsc{gcd}(87, 58) = \textsc{gcd}(58, 29)$

$\triangleright \; 58 = 2 \cdot 29 + 0$

$\textsc{gcd}(58, 29) = \textsc{gcd}(29, 0) = 29$

$\textsc{gcd}(899, 493) = 29$

$29 = 87 - 1 \cdot 58$

$\triangleright \; 58 = 406 - 4 \cdot 87$

$29 = 87 - 1(406 - 4 \cdot 87)$

$\triangleright \; 87 = 493 - 1 \cdot 406$

$29 = 5(493 - 406) - 406$

$\triangleright \; 406 = 899 - 1 \cdot 493$

$29 = 5 \cdot 493 - 6(899 - 493)$

$29 = -6 \cdot 899 + 11 \cdot 493$

$s = -6, \quad t = 11$