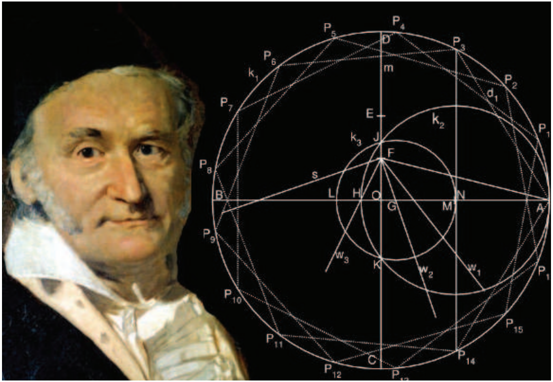
Numbers


P_4
P_5
P_3
D
m
P_6
k_1
P_2
d_1
P_7
E
k_2
P_1
k_3
J
F
P_8
s
B
L
H
O
N
G
M
A
P_9
w_3
K
w_2
w_1
P_{10}
P_{15}
P_{11}
P_{14}
C
P_{12}

Number Systems and Sets

- We represent the set of integers as $\mathcal{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- We denote the set of positive integers modulo n as $\mathcal{Z}_n = \{0, 1, \ldots, n-1\}$
- Elements of $\mathcal{Z}_n$ can be thought of as equivalency classes, where, for $n \geq 2$, every integer in $a \in \mathcal{Z}$ maps into one of the elements $r \in \mathcal{Z}_n$ using the division law $a = q \cdot n + r$ which is represented as $a \equiv r \pmod{n}$
- The symbol $\mathcal{Z}_n^*$ represents the set of positive integers that are less than n and relatively prime to n; if $a \in \mathcal{Z}_n^*$, then $\gcd(a, n) = 1$
- When n is prime, the set would be $\mathcal{Z}_n^* = \{1, 2, \ldots, n-1\}$
- When n is not a prime, the number of elements that are less than n and relatively prime to n is given as $\phi(n) = |\mathcal{Z}_n^*|$

GCD and Euclidean Algorithm

- The greatest common divisor of two integers can be computed using the Euclidean algorithm
- The Euclidean algorithm uses the property

$$\gcd(a, b) = \gcd(b, a - q \cdot b), \quad \text{where} \quad q = \lfloor a/b \rfloor$$

  to reduce the numbers and finally obtains $\gcd(a, b) = \gcd(g, 0) = g$
- For example, to compute $\gcd(56, 21) = 7$, we perform the iterations

$$\begin{array}{rcll} \gcd(56,21) & = & \gcd(21, 56 - 2 \cdot 21) & \text{since} \quad \lfloor 56/21 \rfloor = 2 \\ \gcd(21,14) & = & \gcd(14, 21 - 1 \cdot 14) & \text{since} \quad \lfloor 21/14 \rfloor = 1 \\ \gcd(14,7) & = & \gcd(7, 14 - 2 \cdot 7) & \text{since} \quad \lfloor 14/7 \rfloor = 2 \\ \gcd(7,0) & = & 7 & \end{array}$$

GCD and Euclidean Algorithm

- Given the positive integers a and b with $a > b$, the Euclidean algorithm computes the greatest common divisor g using the code below:

```
while(b != 0) { q = a/b; r = a-q*b; a = b; b = r }
g = a
```

where the division "a/b" operation is the integer division, $q = \lfloor a/b \rfloor$

a	b	q	r	new a	new b
117	45	2	27	45	27
45	27	1	18	27	18
27	18	1	9	18	9
18	9	2	0	9	0
9	0				

Extended Euclidean Algorithm

- Another important property of the GCD is that, if $\gcd(a, b) = g$, then there exists integers s and t such that

$$s \cdot a + t \cdot b = g$$

- We can compute s and t using the extended Euclidean algorithm by working back through the remainders in the Euclidean algorithm, for example, to find $\gcd(833, 301) = 7$, we write

$$\begin{aligned} 833 - 2 \cdot 301 &= 231 \\ 301 - 1 \cdot 231 &= 70 \\ 231 - 3 \cdot 70 &= 21 \\ 70 - 3 \cdot 21 &= 7 \\ 21 - 3 \cdot 7 &= 0 \end{aligned}$$

Extended Euclidean Algorithm

- Since $g = 7$, we start with the 4th equation and plug in the remainder value from the previous equation to this equation, and then move up

$$\begin{aligned}
70 - 3 \cdot (231 - 3 \cdot 70) &= 7 \\
10 \cdot 70 - 3 \cdot 231 &= 7 \\
10 \cdot (301 - 1 \cdot 231) - 3 \cdot 231 &= 7 \\
10 \cdot 301 - 13 \cdot 231 &= 7 \\
10 \cdot 301 - 13 \cdot (833 - 2 \cdot 301) &= 7 \\
-13 \cdot 833 + 36 \cdot 301 &= 7
\end{aligned}$$

Therefore, we find $s = -13$ and $t = 36$ such that $g = 7 = s \cdot a + t \cdot b$

Computation of Multiplicative Inverse

- The extended Euclidean algorithm allows us to compute the multiplicative inverse of an integer a modulo another integer n, if $\gcd(a, n) = 1$
- The EEA obtains the identity $g = s \cdot a + t \cdot b$ which implies

$$\begin{aligned} s \cdot a + t \cdot n &= 1 \\ s \cdot a &= 1 \pmod{n} \\ a^{-1} &= s \pmod{n} \end{aligned}$$

For example, $\gcd(23, 25) = 1$, and the extended Euclidean algorithm returns $s = 12$ and $t = 11$, such that

$$1 = 12 \cdot 23 - 11 \cdot 25$$

therefore $23^{-1} = 12 \pmod{25}$

Fermat's Little Theorem

- Theorem: If p is prime and $\gcd(a,p)=1$, then $a^{p-1}=1 \pmod p$
- For example, $p=7$ and $a=2$, we have $a^{p-1}=2^6=64=1 \pmod 7$
- FLT can be used to compute the multiplicative inverse if the modulus is a prime number

  $$a^{-1}=a^{p-2} \pmod p$$

  since $a^{-1}\cdot a=a^{p-2}\cdot a=a^{p-1}=1 \bmod p$
- The converse of the FLT is not true: If $a^{n-1}=1 \pmod n$ and $\gcd(a,n)=1$, then n may or may not be a prime.
- Example: $\gcd(2,341)=1$ and $2^{340}=1 \pmod{341}$, but 341 is not prime: $341=11\cdot 31$

Euler's Phi Function

- Euler's Phi (totient) Function $\phi(n)$ is defined as the number of numbers in the range $[1, n-1]$ that are relatively prime to n
- Let $n = 7$, then $\phi(7) = 6$ since for all $a \in [1, 6]$, we have $\gcd(a, 7) = 1$
- If p is a prime, $\phi(p) = p - 1$
- For a positive power of prime, we have $\phi(p^k) = p^k - p^{k-1}$
- If n and m are relatively prime, then $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$
- If all prime factors of n is known, then $\phi(n)$ is easily computed:

$$\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Euler's Theorem

- Theorem: If $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1 \pmod{n}$
- Example: $n = 15$ and $a = 2$, we have $2^{\phi(15)} = 2^8 = 256 = 1 \bmod 15$
- Euler's theorem can be used to compute the multiplicative inverse for any modulus:

$$a^{-1} = a^{\phi(n)-1} \pmod{n}$$

  however, this requires the computation of the $\phi(n)$ and therefore the factorization of n
- To compute $23^{-1} \bmod 25$, we need $\phi(25) = \phi(5^2) = 5^2 - 5^1 = 20$, and therefore,

$$23^{-1} = 23^{20-1} = 23^{19} = 12 \pmod{25}$$

Modular Arithmetic Operations

- Given a modulus (prime or composite), how does one compute additions, subtractions, multiplications, and exponentiations?
- $s = a + b \pmod{n}$ is computed in two steps: 1) add, 2) reduce
- If $a, b < n$ to start with, then the reduction step requires a subtraction

$$\text{if} \quad s > n \,, \quad \text{then} \quad s = s - n$$

- $s = a - b \pmod{n}$ is computed similarly: 1) subtract, 2) reduce
- Negative numbers are brought to the range $[0, n-1]$ since we use the least positive representation, e.g., $-5 = -5 + 11 = 6 \pmod{11}$

Modular Multiplication

- $a \cdot b \pmod{n}$ can be computed in two steps: 1) multiply, 2) reduce
- The reduction step requires division by n to get the remainder

$$a \cdot b = s = q \cdot n + r$$

  However, we do not need the quotient!
- The division by n is an expensive operation
- The modular multiplication operation is highly common in public-key cryptography
- The Montgomery Multiplication: An new algorithm for performing modular multiplication that does not require division by n

Modular Exponentiation

- The computation of $a^e \pmod{n}$: Perform the steps of the exponentiation a^e, reducing numbers at each step modulo n
- Exponentiation algorithms: binary method, quaternary method, m-ary methods, power method, sliding windows, addition chains
- The binary method uses the binary expansion of the exponent $e = (e_{k-1} e_{k-2} \cdots e_1 e_0)_2$, and performs squarings and multiplications at each step
- For example, to compute a^{55}, we start with the most significant bit of $e = 55 = (1\ 10111)$, and proceed by scanning the bits

$$a^1 \xrightarrow{s} a^2 \xrightarrow{m} a^3 \xrightarrow{s} a^6 \xrightarrow{s} a^{12} \xrightarrow{m} a^{13} \xrightarrow{s} a^{26} \xrightarrow{m} a^{27} \xrightarrow{s} a^{54} \xrightarrow{m} a^{55}$$

The Binary Method of Exponentiation

- Given the inputs a, n, and $e = (e_{k-1}e_{k-2}\cdots e_1 e_0)_2$, the binary method computes $b = a^e \pmod{n}$ as follows

```
if e[k-1]=1 then b = a else b = 1
for i = k-2 downto 0
    b = b * b mod n
    if e[i] = 1 then b = b * a mod n
return b
```

- For $e = 55 = (110111)$, we have $k = 6$
- Since $e_5 = 1$, we start with $b = a$

	$e_4 = 1$	$e_3 = 0$	$e_2 = 1$	$e_1 = 1$	$e_0 = 1$
Step 2a	$b^2 = a^2$	$b^2 = a^6$	$b^2 = a^{12}$	$b^2 = a^{26}$	$b^2 = a^{54}$
Step 2b	$b \cdot a = a^3$	$b = a^6$	$b \cdot a = a^{13}$	$b \cdot a = a^{27}$	$b \cdot a = a^{55}$

The Chinese Remainder Theorem

- Some cryptographic algorithms work with two (such as RSA) or more moduli (such as secret-sharing) — the Chinese Remainder Theorem (CRT) and underlying algorithm allows to work with multiple moduli
- Theorem: Given k pairwise relatively prime moduli $\{n_i \mid i = 1, 2, \ldots, k\}$, a number $X \in [0, N-1]$ is uniquely representable using the remainders $\{r_i \mid i = 1, 2, \ldots, k\}$ such that $r_i = X \pmod{n_i}$ and $N = n_1 \cdot n_2 \cdots n_k$
  Given the remainders $r_1, r_2, \ldots, r_k$, we can compute X using

$$X = \sum_{i=1}^{k} r_i \cdot c_i \cdot N_i \pmod{N}$$

  where $N_i = N/n_i$ and $c_i = N_i^{-1} \pmod{n_i}$

A CRT Example

- Let the moduli set be $\{5, 7, 9\}$; note that they are pairwise relatively prime $\gcd(5, 7) = \gcd(5, 9) = \gcd(7, 9) = 1$ (even though 9 is not prime)
- We have $n_1 = 5$, $n_2 = 7$, $n_3 = 9$, and thus $N = 5 \cdot 7 \cdot 9 = 315$, therefore, all integers in the range $[0, 314]$ are uniquely representable using these moduli set
- Let $X = 200$, then we have

$$\begin{array}{lllllllll} r_1 & = & 200 \bmod 5 \ ; & r_2 & = & 200 \bmod 7 \ ; & r_1 & = & 200 \bmod 9 \\ r_1 & = & 0 & r_2 & = & 4 & r_3 & = & 2 \end{array}$$

- The remainder set $(0, 4, 2)$ with respect to the moduli set $(5, 7, 9)$ uniquely represents the integer 200, as $\text{CRT}(0, 4, 2; 5, 7, 9) = 200$

A CRT Example

- Compute $Y = \text{CRT}(0, 4, 2; 5, 7, 9)$

$N = n_1 \cdot n_2 \cdot n_3 = 5 \cdot 7 \cdot 9 = 315$

$N_1 = N/n_1 = 315/5 = 7 \cdot 9 = 63$
$N_2 = N/n_2 = 315/7 = 5 \cdot 9 = 45$
$N_3 = N/n_3 = 315/9 = 5 \cdot 7 = 35$

$c_1 = N_1^{-1} = 63^{-1} = 3^{-1} = 2 \pmod{5}$
$c_2 = N_2^{-1} = 45^{-1} = 3^{-1} = 5 \pmod{7}$
$c_2 = N_3^{-1} = 35^{-1} = 8^{-1} = 8 \pmod{9}$

$$\begin{aligned} Y &= r_1 \cdot c_1 \cdot N_1 + r_2 \cdot c_2 \cdot N_2 + r_3 \cdot c_3 \cdot N_3 \pmod{N} \\ &= 0 \cdot 2 \cdot 63 + 4 \cdot 5 \cdot 45 + 2 \cdot 8 \cdot 35 = 1460 \pmod{315} \\ &= 200 \pmod{315} \end{aligned}$$

Therefore, $\text{CRT}(0, 4, 2; 5, 7, 9) = 200$

Another CRT Example

- Compute $Y = \mathrm{CRT}(2, 1, 1; 7, 9, 11)$

$N = n_1 \cdot n_2 \cdot n_3 = 7 \cdot 9 \cdot 11 = 693$

$N_1 = N/n_1 = 693/7 = 9 \cdot 11 = 99$
$N_2 = N/n_2 = 693/9 = 7 \cdot 11 = 77$
$N_3 = N/n_3 = 693/11 = 7 \cdot 9 = 63$

$c_1 = N_1^{-1} = 99^{-1} = 1^{-1} = 1 \pmod 7$
$c_2 = N_2^{-1} = 77^{-1} = 5^{-1} = 2 \pmod 9$
$c_2 = N_3^{-1} = 63^{-1} = 8^{-1} = 7 \pmod{11}$

$$\begin{aligned} Y &= r_1 \cdot c_1 \cdot N_1 + r_2 \cdot c_2 \cdot N_2 + r_3 \cdot c_3 \cdot N_3 \pmod N \\ &= 2 \cdot 1 \cdot 99 + 1 \cdot 2 \cdot 77 + 1 \cdot 7 \cdot 63 = 793 \pmod{693} \\ &= 100 \pmod{693} \end{aligned}$$

Therefore, $\mathrm{CRT}(2, 1, 1; 7, 9, 11) = 100$