Intro. Number Theory

Fermat and Euler

Review

N denotes an n-bit positive integer.   p denotes a prime.

- Z_N = $\{ 0, 1, \ldots, N-1 \}$
- $(Z_N)^*$ = (set of invertible elements in Z_N) =
  = $\{ \; x \in Z_N \; : \; \gcd(x,N) = 1 \; \}$

Can find inverses efficiently using Euclid alg.: time = $O(n^2)$

Fermat's theorem (1640)

Thm: Let p be a prime

$$\forall\, x \in (Z_p)^* : \quad x^{p-1} = 1 \text{ in } Z_p$$

Example: p=5. $3^4 = 81 = 1$ in Z_5

So: $x \in (Z_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ in Z_p

another way to compute inverses, but less efficient than Euclid

Application: generating random primes

Suppose we want to generate a large random prime

say, prime p of length 1024 bits (i.e. $p \approx 2^{1024}$)

Step 1: choose a random integer $p \in [\ 2^{1024}\ ,\ 2^{1025}-1\ ]$

Step 2: test if $2^{p-1} = 1$ in Z_p

If so, output p and stop. If not, goto step 1 .

Simple algorithm (not the best). **$\Pr[\ p \text{ not prime }] < 2^{-60}$**

The structure of $(Z_p)^*$

<u>Thm</u> (Euler): $(Z_p)^*$ is a **cyclic group**, that is

$$\exists \; g \in (Z_p)^* \quad \text{such that} \quad \{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$$

g is called a **<u>generator</u>** of $(Z_p)^*$

Example: $p=7$. $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$

Not every elem. is a generator: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Order

For $g \in (Z_p)^*$ the set $\{1, g, g^2, g^3, \ldots\}$ is called

the **group generated by g**, denoted $<g>$

<u>**Def**</u>: the **order** of $g \in (Z_p)^*$ is the size of $<g>$

$$\text{ord}_p(g) \quad = \quad |<g>| \quad = \quad (\text{smallest } a>0 \text{ s.t. } g^a = 1 \text{ in } Z_p)$$

Examples: $\text{ord}_7(3) = 6$; $\text{ord}_7(2) = 3$; $\text{ord}_7(1) = 1$

<u>**Thm**</u> (Lagrange): $\forall g \in (Z_p)^*$: $\text{ord}_p(g)$ divides $p-1$

Euler's generalization of Fermat (1736)

Def: For an integer N define $\varphi(N) = |(Z_N)^*|$ (Euler's φ func.)

Examples: $\varphi(12) = |\{1,5,7,11\}| = 4$; $\varphi(p) = p-1$

For $N=p\cdot q$: $\varphi(N) = N-p-q+1 = (p-1)(q-1)$

Thm (Euler): $\forall\, x \in (Z_N)^*$: $x^{\varphi(N)} = 1$ in Z_N

Example: $5^{\varphi(12)} = 5^4 = 625 = 1$ in Z_{12}

Generalization of Fermat. Basis of the RSA cryptosystem

End of Segment