Finding a generator of $(Z_p^*, \times)$, or finding a primitive root of $GF(p)$ (short memo)

Hiroshi IMAI

(for the class on April 19)

The order of each element of Z_{13}^*

Multiplicative group $Z_n^* = \{x|\,\mathrm{gcd}(x,n) = 1, 1 \leq x < n\}$

Euler totient function $\phi(n) = |Z_n^*|$

$(Z_p^*,\times), Z_p^* = \{1,2,3,\cdots,p-1\}, p$: prime

Fermat's Theorem: $x^{p-1} \equiv 1 \pmod{p}$, p: prime, $x \in Z_p^*$

Order of $x \in Z_p^*$: $\mathrm{ord}(x) = \min\{k > 0|x^k = 1\}$

E.g., Z_{13}^*, $O_i = \{x|\mathrm{ord}(x) = i\}$

$O_1 = \{1\}, O_2 = \{12\}, O_3 = \{3,9\}, O_4 = \{5,8\}, O_6 = \{4,10\}, O_{12} = \{2,6,7,11\}$

Proposition 1: $|O_k| = \phi(k)$ for k which divides $p-1$.

$\Rightarrow \phi(p-1)$ generators, i.e., $g \in O_{p-1}$: $\{g^i \middle| i = 1,\cdots,p-1\} = Z_p^*$

Randomized Algorithm / Problem

Proposition 2: $\forall n > 1$: $\frac{\phi(n)}{n} = \Omega(\frac{1}{\log n})$. (in fact, $\Omega(\frac{1}{\log \log n})$)

$\Rightarrow$ random sampling from Z_p^* works efficiently

Propositions 3: Given the factorization of $p - 1$, it can be tested whether a given $x \in Z_p^*$ is a generator in polynomial time in $\log n$.

PROBLEM:

1. Find all generators of Z_{17}^*. (mandatory)
2. Prove Propositions 1,2,3. (option)
3. Devise a polynomial-time algorithm to find a generator of Z_p^*, given the factorization of $p - 1$ by using Propositions 1,2,3. (mandatory)

Reports

- Submit your report via ITC-LMS.
- Deadline: July 31, 22:00
- At least submit two reports for obtaining the credits, preferably solving option parts or at least three reports for A