Computer Science & Engineering Department
IIT Kharagpur
Computational Number Theory: CS60094
Lecture IX

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Test for prime II

1.1 Primality by Quadratic Residue

It is known from the *Euler's Criterion* that for an odd prime p, if an integer a is a *quadratic residue* modulo p,[1] then $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. If a is a *quadratic non-residue* modulo p, then $a^{\frac{p-1}{2}} \equiv p-1 \equiv -1 \pmod p$.

Similarly, the Legendre and Jacobi symbol coincides for a prime[2]. $\left(\frac{a}{p}\right) = 1$ if a is a *quadratic residue* modulo p, and is -1 if a is a *quadratic non-residue* modulo p.

We can compute $a^{\frac{p-1}{2}} \bmod n$ by fast exponentiation and we also have efficient algorithm to compute $\left(\frac{a}{n}\right)$.

Proposition 1. If p is an odd prime, then

$$a^{\frac{p-1}{2}} \times \left(\frac{a}{p}\right) \equiv 1 (\text{mod } p) \text{ for all } a \in \mathbb{Z}_p^*.$$

QED.

The equivalent contrapositive statement is

If $n \geq 3$ is an odd integer, $a \in \mathbb{Z}_n^*$ and $a^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right) \not\equiv 1 (\text{mod } n)$, then n cannot be prime.

Example 1. Let $n = 15$. The elements of $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. The values of $\left(\frac{a}{15}\right) \times a^7 \bmod 15$ are as follows:

a	1	2	4	7	8	11	13	14
$\left(\frac{a}{15}\right) \times a^7 \bmod 15$	1	8	4	2	2	4	8	1

So there are large number of witnesses to show that 15 is a composite number.

Definition 1: Let $n \geq 3$ be an odd composite number. An integer $a \in \mathbb{Z}_n$ is called an Euler-witness or E-witness for n if $(a^{\frac{n-1}{2}} \bmod n) \times \left(\frac{a}{n}\right) \neq 1$. Otherwise it is called an E-liar,

$$L_n^E = \{a \in \mathbb{Z}_n^* : \left(a^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right)\right) \equiv 1 (\text{mod } n)\}.$$

Example 2. Consider $n = 225$ and $a = 26$. We have $26^{\frac{225-1}{2}} \bmod 225 = 26^{112} \bmod 225 = 1$ and

$$\left(\frac{26}{225}\right) = \left(\frac{13}{15^2}\right)\left(\frac{2}{15^2}\right) = 1.$$

So 26 is an E-liar for the composite 225. But $2^{112} \bmod 225 = 196$, so 2 is an E-witness of compositeness of 225.

A few other *E-liars* for 225 are 82, 107, 118, 143 etc.

Proposition 2. Let $n \geq 3$ be an odd composite number. Then every E-liar for n is also an F-liar for n. QED.

[1] $p \not| a$ and a is a *perfect square* modulo p.

[2] We have seen that for a composite number n, $\left(\frac{a}{n}\right) = 1$ does not mean that a is a quadratic residue modulo n. As an example $\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right) = (-1) \times (-1) = 1$. But There is no solution of $x^2 \equiv 3(\text{mod } 35)$.

Proof: Let a be an E-liar for n. So $a^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right) \equiv 1 \pmod{n}$. The value of $\left(\frac{a}{n}\right) \in \{1, -1\}$ (it cannot be equal to 0 as the product is congruent to 1). So the value of

$$\left(a^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right)\right)^2 \equiv 1 \pmod{n}.$$

The value of $\left(\frac{a}{n}\right)^2 = 1$, implies that $a^{n-1} \equiv 1 (\bmod\ n)$ i.e. a is an F-liar for n. QED.

If $L_n^E \subseteq L_n^F$, then an F-witness of n is also an E-witness of n i.e. $W_n^F \subseteq W_n^E$.

We prove that more than half of the elements of $\mathbb{Z}_n^*$ are E-witnesses.

Proposition 3. Let $n \geq 3$ be an odd composite number. The set of E-liars of n, L_n^E, is a *proper subgroup* of $\mathbb{Z}_n^*$. QED.

Proof: We know $L_n^E \subseteq L_n^F \subseteq \mathbb{Z}_n^*$. We prove that L_n^E is closed under the group operation.

Let $a, b \in L_n^E$.

$$(a \cdot b)^{\frac{n-1}{2}} \times \left(\frac{a \cdot b}{n}\right) \equiv \left(a^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right)\right) \cdot \left(b^{\frac{n-1}{2}} \times \left(\frac{b}{n}\right)\right) \equiv 1 \cdot 1 \equiv 1 (\bmod\ n).$$

Finally we show that all elements of $\mathbb{Z}_n^*$ are not E-liars. There is at least one E-witness in $\mathbb{Z}_n^*$. This will imply L_n^E is a proper subgroup. We consider two cases.

Case I: Let $n = p^k \cdot m$, where p is an odd prime, $k \geq 2$ and m is an odd number relatively prime to p.

(a) If $m = 1$, we choose $a = p + 1$ and claim that a is an F-witness of n. So it is also an E-witness of n.

$gcd(a, n) = gcd(p + 1, p^k) = 1$ implies that $a \in \mathbb{Z}_n^*$. Now we show that a is an F-witness.

If a is an F-liar, then $a^{n-1} \equiv 1 \pmod{n}$, implies that $a^{n-1} \equiv 1 \pmod{p^2}$ as p^2 is a divisor of n. So we have

$$a^{n-1} \equiv (1+p)^{n-1} \equiv 1 + (n-1)p + \sum_{2 \leq i \leq n-1} \binom{n-1}{i} p^i \equiv 1 + (n-1)p \pmod{p^2}.$$

$p^2 | a^{n-1} - 1$, so $p^2 | (n-1)p$. Hence $p | n - 1$. But that is impossible as $p | n$. So a is an E-witness.

(b) If $m \geq 3$, we take a as a solution of the pair of congruence

$$\begin{aligned} x &\equiv 1 + p \pmod{p^2}, \\ x &\equiv 1 \pmod{m} \end{aligned}$$

By the CRT there is a solution a, $1 \leq a < p^2 \cdot m \leq n$.

As $a \equiv 1 + p \pmod{p^2}$, $a \equiv 1 + p \pmod{p}$, implies that $p | a - 1$. Hence $gcd(a, p^k) = 1$.

Similarly, $m | a - 1$, so $gcd(a, m) = 1$. As $n = p^k \cdot m$, the value of $gcd(a, n)$ cannot be larger than 1. Hence $a \in \mathbb{Z}_n^*$.

Our proof that this a cannot be an F-liar is similar to the case of $m = 1$.

Case II: n may be square-free and is a product of several distinct primes. Let $n = p \cdot m$ where p is an odd prime and $m \geq 3$ is an odd square free integer so that $p \not| m$.

Let $b \in \mathbb{Z}_p^*$ be a *quadratic non-residue* modulo p i.e. $\left(\frac{b}{p}\right) = -1$. We consider the following congruence

$$\begin{aligned} x &\equiv b \pmod{p}, \\ x &\equiv 1 \pmod{m}. \end{aligned}$$

By CRT there is a solution a of this pair of congruence, $1 \leq a < p \cdot m = n$. We prove that $a \in \mathbb{Z}_n^*$ and a is an E-witness.

$p | a - b$ and $1 \leq b < p$, so $p \not| a$. Also $gcd(a, m) = 1$, hence $gcd(a, n) = gcd(a, p \cdot m) = 1$. So $a \in \mathbb{Z}_n^*$. We also have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{m}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{1}{m}\right) = -1 \cdot 1 = -1.$$

If a is an E-liar, then $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. On the other hand m is a divisor of n, so $a^{\frac{n-1}{2}} \equiv -1 \pmod{m}$. But that contradicts the fact that $a \equiv 1 \pmod{m}$. So a is an E-witness of n. QED.

The size of E-liar is $\leq \frac{\phi(n)}{2} \leq \frac{n-2}{2}$. So at least half of the elements of $\mathbb{Z}_n^*$ are E-witnesses.

1.2 Solovay-Strassen Test

R. Solovay and V. Strassen proposed the following *randomized* test in 1977.

isprimeSS(n) // n is odd ≥ 3
  a $\leftarrow$ *rand*$\{2, \cdots, n-2\}$
  `if` a$^{\frac{n-1}{2}} \times \left(\frac{a}{n}\right) \bmod n \neq 1$
    `return 0`
  `return 1`

References

[AB] *Computational Number Theory* by Abhijit Das, (will be published from CRC Press).

[CLR] *Introduction to Algorithms* by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, 2nd ed., Pub. Pub. PHI, 2001, ISBN 81-203-2141-3.

[MD] *Primality Testing in Polynomial Time From Randomized Algorithms to "PRIMES is in P"* by Martin Dietzfelbinger, LNCS 3000, Pub. Springer, 2004, ISBN 3-540-40344-2.

[VS] *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, 2nd ed., Pub. Cambridge University Press, 2009, ISBN 978-0-521-51644-0.