Complexity and Cryptography

Thomas Zeugmann

Hokkaido University
Laboratory for Algorithmics

https://www-alg.ist.hokudai.ac.jp/~thomas/COCRB/

Lecture 5: Testing Primality and Taking Discrete Roots

Legendre Symbol

It advantageous to introduce the following notions: Let p be an odd prime, and let $a \in \mathbb{Z}_p^*$. We say that a is a *quadratic residue* modulo p if $x^2 \equiv a \mod p$ is solvable in $\mathbb{Z}_p^*$. If a is not a quadratic residue modulo p, then we call a a *quadratic nonresidue*. The following symbol was introduced by Adrien-Marie Legendre.

Definition 1 (Legendre Symbol)

We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) =_{df} \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p\,; \\ -1, & \text{otherwise.} \end{cases}$$

Quadratic Residues I

The following theorem is needed below:

Theorem 1

Let p be an odd prime and let $g \in \mathbb{Z}_p^*$ be a generator for $\mathbb{Z}_p^*$. Then for all $a \in \mathbb{Z}_p^*$ we have: a is a quadratic residue modulo p if and only if $\mathrm{dlog}_g\, a$ is even.

Quadratic Residues I

The following theorem is needed below:

Theorem 1

Let p be an odd prime and let $g \in \mathbb{Z}_p^*$ be a generator for $\mathbb{Z}_p^*$. Then for all $a \in \mathbb{Z}_p^*$ we have: a is a quadratic residue modulo p if and only if $\mathrm{dlog}_g\, a$ is even.

Proof. Sufficiency. Let $a \equiv g^{2m} \mod p$ for some $m > 0$. Then, $b =_{df} g^m \mod p$ is obviously a solution of $x^2 \equiv a \mod p$. Thus a is a quadratic residue modulo p.

Quadratic Residues I

The following theorem is needed below:

Theorem 1

Let p be an odd prime and let $g \in \mathbb{Z}_p^*$ be a generator for $\mathbb{Z}_p^*$. Then for all $a \in \mathbb{Z}_p^*$ we have: a is a quadratic residue modulo p if and only if $\mathrm{dlog}_g\, a$ is even.

Proof. Sufficiency. Let $a \equiv g^{2m} \mod p$ for some $m > 0$. Then, $b =_{df} g^m \mod p$ is obviously a solution of $x^2 \equiv a \mod p$. Thus a is a quadratic residue modulo p.

Necessity. Let b be a solution of $x^2 \equiv a \mod p$, and let $m = \mathrm{dlog}_g\, b$, i.e., $b \equiv g^m \mod p$. Thus, $a \equiv g^{2m} \mod p$. By Fermat's Little Theorem we have $\mathrm{dlog}_g\, a \equiv 2m \mod (p-1)$.

Since $2|(p-1)$, we can conclude $2|\mathrm{dlog}_g\, a$, too. ∎

Quadratic Residues II

The latter theorem directly implies the following corollaries:

Corollary 1

Let p be an odd prime. Then there are precisely $(p-1)/2$ many quadratic residues and $(p-1)/2$ many quadratic nonresidues in $\mathbb{Z}_p^*$.

Corollary 2

Let p be an odd prime. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all $a, b \in \mathbb{Z}_p^*$.

Furthermore, we need the following theorem:

Quadratic Residues II

The latter theorem directly implies the following corollaries:

Corollary 1

Let p be an odd prime. Then there are precisely $(p-1)/2$ many quadratic residues and $(p-1)/2$ many quadratic nonresidues in $\mathbb{Z}_p^*$.

Corollary 2

Let p be an odd prime. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all $a, b \in \mathbb{Z}_p^*$.

Furthermore, we need the following theorem:

Theorem 2

Let p be an odd prime and let g be a generator of $\mathbb{Z}_p^*$. Then we have $g^{(p-1)/2} \equiv -1 \mod p$.

©Thomas Zeugmann

Quadratic Residues III

Proof. Consider $x^2 \equiv 1 \mod p$. Obviously, 1 and -1 are solutions of $x^2 \equiv 1 \mod p$. By Lemma 4.1, we know that there are no other solutions.
By Fermat's Little Theorem we have

$$\left(g^{(p-1)/2}\right)^2 \equiv g^{p-1} \equiv 1 \mod p\ .$$

Thus, $g^{(p-1)/2}$ is a solution of $x^2 \equiv 1 \mod p$.

Since g is a generator, we have $g^{(p-1)/2} \not\equiv 1 \mod p$. Therefore, $g^{(p-1)/2} \equiv -1 \mod p$ must hold. ∎

Quadratic Residues IV

The following theorem provides one way to compute the Legendre symbol. It was found by Leonhard Euler.

Theorem 3 (Euler's Criterion)

Let p be an odd prime and let $a \in \mathbb{Z}_p^*$, then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p\,.$$

Quadratic Residues V

Proof. We distinguish the following cases:

Case 1. $\left(\frac{a}{p}\right) = 1$.

So, there exists a $b \in \mathbb{Z}_p^*$ such that $b^2 \equiv a \mod p$. Thus, by Theorem 2 from Lecture 3 and Fermat's Little Theorem we have

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p \ .$$

Quadratic Residues V

Proof. We distinguish the following cases:

Case 1. $\left(\dfrac{a}{p}\right) = 1\,.$

So, there exists a $b \in \mathbb{Z}_p^*$ such that $b^2 \equiv a \mod p$. Thus, by Theorem 2 from Lecture 3 and Fermat's Little Theorem we have

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p\,.$$

Case 2. $\left(\dfrac{a}{p}\right) = -1\,.$

Let g be a generator of $\mathbb{Z}_p^*$. Then $a \equiv g^{2m+1} \mod p$ for some $m \in \mathbb{N}$, since a is a quadratic residue modulo p if and only if the discrete logarithm of a (wrt. g) is even (cf. Theorem 1). Hence, using Theorem 2 we get

$$\begin{aligned} a^{(p-1)/2} &\equiv g^{(2m+1)(p-1)/2} \equiv g^{m(p-1)} g^{(p-1)/2} \\ &\equiv 1 \cdot (-1) \equiv -1 \mod p\,. \end{aligned}$$

$\blacksquare$

Jacobi Symbol

The following definition generalizes in some sense the Legendre symbol, but *not* with respect to the existence of discrete square roots. Still, it provides enough information to design an efficient probabilistic test for primality. This generalization was introduced by Carl Jacobi.

©Thomas Zeugmann

Jacobi Symbol

The following definition generalizes in some sense the Legendre symbol, but *not* with respect to the existence of discrete square roots. Still, it provides enough information to design an efficient probabilistic test for primality. This generalization was introduced by Carl Jacobi.

Definition 2 (Jacobi Symbol)

Let $Q > 1$ be an odd number, and let $Q = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, where p_i prime for all $i = 1, \ldots, k$ (but not necessarily $p_i \neq p_j$ for $i \neq j$). Let $a \in \mathbb{Z}_Q^*$. The *Jacobi symbol* $\left(\frac{a}{Q}\right)$ is defined as follows:

$$\left(\frac{a}{Q}\right) =_{df} \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \cdots \cdot \left(\frac{a}{p_k}\right) .$$

Jacobi Symbol

The following definition generalizes in some sense the Legendre symbol, but *not* with respect to the existence of discrete square roots. Still, it provides enough information to design an efficient probabilistic test for primality. This generalization was introduced by Carl Jacobi.

Definition 2 (Jacobi Symbol)

Let $Q > 1$ be an odd number, and let $Q = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, where p_i prime for all $i = 1, \ldots, k$ (but not necessarily $p_i \neq p_j$ for $i \neq j$). Let $a \in \mathbb{Z}_Q^*$. The *Jacobi symbol* $\left(\frac{a}{Q}\right)$ is defined as follows:

$$\left(\frac{a}{Q}\right) =_{df} \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \cdots \cdot \left(\frac{a}{p_k}\right) .$$

Example: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = 1$ but $x^2 \equiv 2 \mod 15$ is *not* solvable in $\mathbb{Z}_{15}^*$.

Solovay and Strassen's Primality Test I

Now, we turn our attention to a probabilistic algorithm for testing primality. We shall arrive at a *Monte Carlo* algorithm; i.e., a randomized procedure that may produce incorrect results but with a bounded error probability. A formal definition of the relevant complexity class will be provided later.

The following result is due to Solovay and Strassen (1977):

Solovay and Strassen's Primality Test I

Now, we turn our attention to a probabilistic algorithm for testing primality. We shall arrive at a *Monte Carlo* algorithm; i.e., a randomized procedure that may produce incorrect results but with a bounded error probability. A formal definition of the relevant complexity class will be provided later.

The following result is due to Solovay and Strassen (1977):

Theorem 4

Testing primality can be done in one-sided error probabilistic polynomial time.

Solovay and Strassen's Primality Test II

Let $n \in \mathbb{N}$ be any given number. Clearly, if n is even, this can be trivially recognized. Thus, it suffices to show how to recognize odd primes. Consider the following algorithm:

Algorithm PT

Input: An odd number $n \in \mathbb{N}$.

Method: (1) Choose at random a number $a \in \{1, \ldots, n-1\}$.

(2) Compute $d = \gcd(a, n)$. If $d > 1$ then output *composite*, and stop. Otherwise, goto (3).

(3) Compute the following quantities:

$\delta = a^{(n-1)/2} \mod n$;

$\varepsilon = \left(\frac{a}{n}\right)$ (the Jacobi symbol).

Output: If $\delta \not\equiv \varepsilon \mod n$ then output *composite*, and stop.
If $\delta \equiv \varepsilon \mod n$ then output *possibly prime*, and stop.

Solovay and Strassen's Primality Test III

Next, we prove two lemmata which will yield the statement of the theorem.

Solovay and Strassen's Primality Test III

Next, we prove two lemmata which will yield the statement of the theorem.

Lemma 1. *If n is prime, then Algorithm* **PT** *must output* possibly prime.

If n is prime then $\gcd(a, n) = 1$ for all $a \in \{1, \ldots, n-1\}$, and by Theorem 3,

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \mod n\,.$$

Thus, the Algorithm **PT** necessarily outputs "possibly prime."

Solovay and Strassen's Primality Test IV

Lemma 2. *If n is composite, then Algorithm* **PT** *outputs* composite *with probability at least* $1/2$.

The main ingredient for proving this lemma is the following claim:

Solovay and Strassen's Primality Test IV

Lemma 2. *If n is composite, then Algorithm* **PT** *outputs* composite *with probability at least* $1/2$.

The main ingredient for proving this lemma is the following claim:

Claim 1. *Let $n \in \mathbb{N}$ be an odd composite number. Then we have for*

$$S =_{df} \left\{ a \in \mathbb{Z}_n^* \mid a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n \right\} \text{ that } |S| \leqslant |\mathbb{Z}_n^*|/2\,.$$

Proof of Claim 1

Note that S is a subgroup of $\mathbb{Z}_n^*$, since it is closed under multiplication. This follows from the identity $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ for the Jacobi symbol. Thus, $|S|$ must divide $|\mathbb{Z}_n^*|$, and hence either

$$|S| = |\mathbb{Z}_n^*| \quad \text{or} \quad |S| \leqslant |\mathbb{Z}_n^*|/2\,.$$

So it suffices to show that $|S| \neq |\mathbb{Z}_n^*|$.

©Thomas Zeugmann

Proof of Claim 1

Note that S is a subgroup of $\mathbb{Z}_n^*$, since it is closed under multiplication. This follows from the identity $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ for the Jacobi symbol. Thus, $|S|$ must divide $|\mathbb{Z}_n^*|$, and hence either

$$|S| = |\mathbb{Z}_n^*| \quad \text{or} \quad |S| \leqslant |\mathbb{Z}_n^*|/2\,.$$

So it suffices to show that $|S| \neq |\mathbb{Z}_n^*|$.

Suppose that $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \mod n$ for all $a \in \mathbb{Z}_n^*$. Since $\left(\frac{a}{n}\right) = \pm 1$, we conclude $a^{n-1} \equiv 1 \mod n$ for all $a \in \mathbb{Z}_n^*$, thus n must be a Carmichael number. By our results from Lecture 4, n must be square-free and n must be the product of at least three different primes.

Proof of Claim 1

Therefore,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \dots \cdot \left(\frac{a}{p_k}\right) ,$$

where $p_1, \dots, p_k$ are prime numbers and $k \geqslant 3$. Let g be a generator for $\mathbb{Z}^*_{p_1}$, and let $\tilde{n} = n/p_1$. By the Chinese remainder theorem there exists an $a \in \mathbb{Z}^*_n$ such that

$$\begin{aligned} a &\equiv g \mod p_1 , && (1)\\ a &\equiv 1 \mod \tilde{n} . && (2) \end{aligned}$$

In particular, we therefore have $a \equiv 1 \mod p_j$ for all $j \geqslant 2$, and hence a is quadratic residue modulo p_j for all $j \geqslant 2$.

Proof of Claim 1

Thus, $\left(\frac{a}{p_j}\right) = 1$ for all $j \geqslant 2$. Moreover, by Theorems 2 and 3, we obtain from (1) that

$$a^{(p_1-1)/2} \equiv g^{(p_1-1)/2} \equiv -1 \equiv \left(\frac{a}{p_1}\right) \mod p_1 \,.$$

Consequently, $\left(\frac{a}{n}\right) = -1$, too, and therefore (cf. Definition of S)

$$a^{(n-1)/2} \equiv -1 \mod n \,.$$

This implies $a^{(n-1)/2} \equiv -1 \mod \tilde{n}$. By (2) we have $a \equiv 1 \mod \tilde{n}$, and hence $a^{(n-1)/2} \equiv 1 \mod \tilde{n}$. This contradiction shows that $S = \mathbb{Z}_n^*$ is impossible. Thus Claim 1 is shown.

©Thomas Zeugmann

Solovay and Strassen's Primality Test V

Now, if n is composite, then with probability 1/2 the Algorithm **PT** chooses an $a \in \{1, \ldots, n-1\}$ such that

$$\delta \not\equiv \varepsilon \mod n\,,$$

and therefore, with probability at least 1/2 the output is *composite*.
This proves the correctness of the Algorithm **PT**.

It remains to evaluate the running time of Algorithm **PT**.
Everything is clear except the calculation of the Jacobi symbol.
If the Jacobi symbol can be computed in polynomial time (as shown below), we are done. ∎

Law of Quadratic Reciprocity

So, it remains to provide an effective method for computing the Jacobi symbol. We cannot reduce the computation of the Jacobi symbol to its definition, since this would require that we know the prime factorization of n. But there is a very nice method which is based on the following theorem and its supplement.

Theorem 5 (Law of Quadratic Reciprocity)

For all odd numbers $P, Q \in \mathbb{N}$ *with* $\gcd(Q, P) = 1$ *we have*

$$\left(\frac{Q}{P}\right) = (-1)^{(P-1)(Q-1)/4}\left(\frac{P}{Q}\right) .$$

Because of the lack of time, we do not prove this theorem here. There are numerous proofs in print. The first rigorous proof has been given by Gauß.

©Thomas Zeugmann

Supplements

To apply Theorem 5, we need the following supplements:

Theorem 6

For all $a, b \in \mathbb{N}$ *and all odd* $Q \in \mathbb{N}$ *we have*

(1) *if* $a \equiv b \mod Q$ *then* $\left(\frac{a}{Q}\right) = \left(\frac{b}{Q}\right)$ *;*

(2) $\left(\frac{1}{Q}\right) = 1$ *;*

(3) $\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2}$ *;*

(4) $\left(\frac{ab}{Q}\right) = \left(\frac{a}{Q}\right) \cdot \left(\frac{b}{Q}\right)$ *;*

(5) $\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$.

Solovay and Strassen's Primality Test VI

So, the complexity of computing the Jacobi symbol is of the same order as the complexity of the extended Euclidean algorithm. Let us compute $\left(\frac{117}{739}\right)$.

$$\begin{aligned}
\left(\frac{117}{739}\right) &= +\left(\frac{739}{117}\right) && (*\text{Theorem } 5*) \\
&= +\left(\frac{37}{117}\right) && (*\text{Theorem } 6, (1)*) \\
&= +\left(\frac{117}{37}\right) = \left(\frac{6}{37}\right) \\
&= +\left(\frac{2\cdot 3}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{3}{37}\right) \\
&= -\left(\frac{3}{37}\right) && (*\text{Theorem } 6, (5)*) \\
&= -\left(\frac{37}{3}\right) = -\left(\frac{1}{3}\right) = -1\,.
\end{aligned}$$

Solovay and Strassen's Primality Test VII

We provide a method for improving the error probability of the Solovay-Strassen algorithm exponentially.

Corollary 3

If we run the algorithm **PT** k*-times then*

$$\Pr\{k \text{ successive runs output "possibly prime"}\} \leqslant \frac{1}{2^k}$$

provided n *is composite.*

Proof. As we have seen, a composite number may lead to the wrong output *possibly prime* with probability $\leqslant 1/2$. Thus, if we run the algorithm **PT** k-times we have k independent Bernoulli trials with failure probability $1/2$. Hence,

$$\Pr\{k \text{ successive runs output "possibly prime"}\} \leqslant \frac{1}{2^k}\ ,$$

since it equals the probability of k successive failures. ∎

Remark

This is a good place to return to the problem of computing discrete roots. We study Berlekamp's algorithm for computing discrete square roots modulo a *prime number*. In general, however, the problem of finding discrete square roots must be considered to be difficult. As a matter of fact, one can prove that finding the *least* solution of $x^2 \equiv a \mod n$ in positive integers, where $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$, is an $\mathcal{NP}$-hard problem.

Remark

This is a good place to return to the problem of computing discrete roots. We study Berlekamp's algorithm for computing discrete square roots modulo a *prime number*. In general, however, the problem of finding discrete square roots must be considered to be difficult. As a matter of fact, one can prove that finding the *least* solution of $x^2 \equiv a \mod n$ in positive integers, where $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$, is an $\mathcal{NP}$-hard problem.

Next, we explain what is meant by *Las Vegas* algorithm. A randomized procedure is called Las Vegas algorithm, if the procedure always correctly computes the desired result (that is, independently from the random choices made). The run time of the procedure, however, does depend on the random choices made. Then, the time complexity of a Las Vegas algorithm on input X is defined to be the expected value with respect to all possible random choices.

Berlekamp's Algorithm I

Theorem 7

Let $p \in \mathbb{N}$ be an odd prime and let $a \in \mathbb{Z}_p^*$. Then there is a Las Vegas algorithm to find all solutions of

$$x^2 \equiv a \mod p\,.$$

Berlekamp's Algorithm II

Proof. Consider the following Algorithm **BA**:

Input: *An odd prime* p *and an* $a \in \mathbb{Z}$ *such that* $\gcd(a, p) = 1$.

Output: **no solutions** *if* a *is a quadratic nonresidue modulo* p; *all solutions of* $x^2 \equiv a \mod p$, *if* a *is a quadratic residue modulo* p.

Method:

(1) Compute $\left(\frac{a}{p}\right)$; if $\left(\frac{a}{p}\right) = 1$ then goto (2). Otherwise, output **no solutions**, and stop.

(2) Choose randomly a $\gamma \in \mathbb{Z}_p^*$ until a number γ has been found such that $\left(\frac{\gamma^2 - a}{p}\right) = -1$. Compute $\left(x^{\frac{p-1}{2}} - 1\right) \mod ((x-\gamma)^2 - a)$, and let $\delta(x - \rho)$ be the result of this computation. Output $(\rho - \gamma)$ and $-(\rho - \gamma)$, and stop.

Example

Let us consider the following example, where the input is $p = 17$ and $a = 8$:
Since

$$\left(\frac{8}{17}\right) \equiv 8^8 \equiv (-4)^4 \equiv (-1)^2 \equiv 1 \mod 17\,,$$

we see that $x^2 \equiv 8 \mod 17$ is solvable.
Now, we choose $\gamma = 6$ and easily verify

$$\begin{aligned}\left(\frac{\gamma^2 - a}{p}\right) &= \left(\frac{36-8}{17}\right) = \left(\frac{28}{17}\right) = \left(\frac{11}{17}\right)\\ &\equiv 11^8 \equiv 121^4 \equiv 2^4 \equiv -1 \mod 17\,.\end{aligned}$$

Example continued

Next, we have to compute $(x^8 - 1) \mod ((x-6)^2 - 8)$. As an easy but somehow tedious computation shows, the result is

$$6521856x - 20674305 \equiv 10x - 10 \equiv 10(x-1) \mod 17\,.$$

Therefore, $\delta = 10$ and $\rho = 1$. Consequently, we output -5 and 5.

 ©Thomas Zeugmann

Example continued

Note that, in general, one has to do a bit more for getting δ and ρ. To see this, let us have a look at another computation arising by choosing $\gamma = 8$ instead of 6.

$$\begin{aligned}\left(\frac{\gamma^2 - a}{p}\right) &= \left(\frac{64-8}{17}\right) = \left(\frac{56}{17}\right) = \left(\frac{5}{17}\right) \\ &\equiv 5^8 \equiv 390625 \equiv -1 \mod 17\,, \text{ and get}\end{aligned}$$

$$\begin{aligned}(x^8 - 1) \mod ((x-8)^2 - 8) &= 33325056x - 171831277 \\ &\equiv 7x - 6 \mod 17\,.\end{aligned}$$

So, we have to compute the *modular inverse* of 7 modulo 17, which is 5 and get $\delta = 7$ and $\rho = 13$, since

$$7x - 6 \equiv 7x - 6 \cdot \underbrace{7 \cdot 5}_{\equiv 1 \mod 17} \equiv 7(x - 6 \cdot 5) \equiv 7(x - 13) \mod 17.$$

Berlekamp's Algorithm III

First, we prove the correctness of the procedure given above.

Obviously, if a is a quadratic nonresidue modulo p than the Legendre symbol evaluates to -1, and thus the Algorithm **BA** is correct.

Next, we assume a to be a quadratic residue modulo p. Hence, the Legendre symbol evaluates to 1, and Instruction (2) is executed.

Berlekamp's Algorithm III

First, we prove the correctness of the procedure given above. Obviously, if a is a quadratic nonresidue modulo p than the Legendre symbol evaluates to -1, and thus the Algorithm **BA** is correct.

Next, we assume a to be a quadratic residue modulo p. Hence, the Legendre symbol evaluates to 1, and Instruction (2) is executed. Suppose, we have found a number γ such that $\left(\frac{\gamma^2-a}{p}\right) = -1$. Taking into account that $x^2 \equiv a \mod p$ is solvable, we may conclude that

$$(x-\gamma)^2 - a \equiv 0 \mod p \tag{3}$$

is solvable, too. This is obvious, if we look at $x-\gamma$ as a new variable. In particular, this statement does not depend on the choice of γ. The choice of γ, however, is important for deriving useful information as we shall see in Claim 1 below.

©Thomas Zeugmann

Berlekamp's Algorithm IV

Let ρ and σ be the solutions of $(x-\gamma)^2 \equiv a \mod p$, i.e., we have

$$\begin{aligned}(\rho-\gamma)^2 - a &\equiv 0 \mod p\ ,\\ (\sigma-\gamma)^2 - a &\equiv 0 \mod p\ .\end{aligned}$$

Next, we prove a very helpful claim.

Claim 1. $\rho\cdot\sigma \equiv \gamma^2 - a \mod p\ .$

$\rho \cdot \sigma \equiv \gamma^2 - a \mod p$

We have the congruence $z^2 - a \equiv 0 \mod p$, where $z = (x - \gamma)$. By Eq. (3), we know that this congruence has precisely two solutions, say $z_1,\ z_2$. Using $z_1 \equiv -z_2 \mod p$ we may conclude

$$z_1 \cdot z_2 \equiv -z_1 \cdot z_1 \equiv -z_1^2 \equiv -a \mod p\ .$$

Thus, $z_1 \cdot z_2 \equiv -a \mod p$. So, $z_1 = (\rho - \gamma)$ and $z_2 = (\sigma - \gamma)$.

$(\rho - \gamma)(\sigma - \gamma) \equiv -a \mod p$, therefore, we get

$$\rho\sigma - \gamma\sigma - \gamma\rho + \gamma^2 \equiv -a \mod p\ . \tag{4}$$

$\rho \cdot \sigma \equiv \gamma^2 - a \mod p$

We have the congruence $z^2 - a \equiv 0 \mod p$, where $z = (x - \gamma)$. By Eq. (3), we know that this congruence has precisely two solutions, say $z_1,\ z_2$. Using $z_1 \equiv -z_2 \mod p$ we may conclude

$$z_1 \cdot z_2 \equiv -z_1 \cdot z_1 \equiv -z_1^2 \equiv -a \mod p\,.$$

Thus, $z_1 \cdot z_2 \equiv -a \mod p$. So, $z_1 = (\rho - \gamma)$ and $z_2 = (\sigma - \gamma)$.

$$(\rho - \gamma)(\sigma - \gamma) \equiv -a \mod p\,, \text{therefore, we get}$$

$$\rho\sigma - \gamma\sigma - \gamma\rho + \gamma^2 \equiv -a \mod p\,. \tag{4}$$

Now, $\rho - \gamma \equiv -\sigma + \gamma \mod p$, and thus $-\sigma \equiv \rho - 2\gamma \mod p$. Consequently, we obtain from (4):

$$\begin{aligned} \rho\sigma + \gamma(\rho - 2\gamma) - \gamma\rho + \gamma^2 &\equiv -a \mod p \\ \rho\sigma + \gamma\rho - 2\gamma^2 - \gamma\rho + \gamma^2 &\equiv -a \mod p \\ \rho\sigma &\equiv \gamma^2 - a \mod p\,. \end{aligned}$$

∎(Claim 1)

Berlekamp's Algorithm V

Taking into account that $\left(\frac{\rho\sigma}{p}\right) = \left(\frac{\rho}{p}\right)\left(\frac{\sigma}{p}\right)$, and $\left(\frac{\gamma^2 - a}{p}\right) = -1$, we conclude that $\left(\frac{\rho}{p}\right) = -\left(\frac{\sigma}{p}\right)$. Without loss of generality, let $\left(\frac{\rho}{p}\right) = 1$. Then, $(x - \rho)$ is a factor of $x^{(p-1)/2} - 1$ modulo p while $(x - \sigma)$ is not. This follows directly from the Euler criterion, since $\rho^{(p-1)/2} \equiv 1 \mod p$, and thus ρ is a root of the polynomial $x^{(p-1)/2} - 1$ over $\mathbb{Z}_p$.

Berlekamp's Algorithm VI

Consequently,

$$\gcd\big((x-\gamma)^2 - a,\, x^{(p-1)/2} - 1\big) = (x-\rho),$$

since ρ and σ are the only solutions of $(x-\gamma)^2 - a \equiv 0 \mod p$. Hence,

$$\big(x^{(p-1)/2} - 1\big) \mod (x-\gamma)^2 - a$$

is a polynomial of degree 1 which can be written as $\delta(x-\rho)$. Finally, as we have seen, $(\rho-\gamma)$ is a discrete root of a modulo p. Since there are precisely two roots, $-(\rho-\gamma)$ is the only other solution. This proves the correctness.

Berlekamp's Algorithm VII

Finally, we have to deal with the question of finding γ such that $\left(\frac{\gamma^2-a}{p}\right) = -1$. Note that if $p \equiv 3 \mod 4$ then $\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right) = -1$. Thus, in this case the choice $\gamma = 0$ will always succeed and no randomization is needed.
The remaining case is handled by the following lemma:

Lemma 1

Let $p \in \mathbb{N}$ be prime satisfying $p \equiv 1 \mod 4$ and let $a \in \mathbb{Z}_p^*$ be such that $\left(\frac{a}{p}\right) = 1$. Then at most half of the elements of $\gamma \in \mathbb{Z}_p^*$ satisfy the condition $\left(\frac{\gamma^2-a}{p}\right) = 1$.

Berlekamp's Algorithm VIII

Thus, in case of $p \equiv 1 \mod 4$ the expected number of random choices required in (2) is bounded by 2.

Obviously, all computations in (1) can be done in time polynomial in the lengths of p and a and so can the computation of $\left(\frac{\gamma^2 - a}{p}\right)$ in (2) until an appropriate γ is found.

Finally, the computation of

$$\left(x^{(p-1)/2} - 1\right) \mod \left((x - \gamma)^2 - a\right)$$

can be done by successively squaring x and reducing it modulo $\left((x - \gamma)^2 - a\right)$ as in the computation of $a^m \mod n$ outlined in Algorithm **EXP**. ∎

Proof of the Lemma I

We need the following claim:

Claim 2. Let p *be a prime number such that* $p \equiv 1 \mod 4$ *and let* g *be a generator for* $\mathbb{Z}_p^*$*. Furthermore, for* $i, j \in \{0, 1\}$ *let*

$$\begin{aligned} S_{ij} \quad =_{df} \quad & \{(x, y) \mid \ x, y \in \mathbb{Z}_{p-1} \text{ and } x \equiv i \bmod 2,\ y \equiv j \bmod 2 \\ & \text{and } g^x + 1 \equiv g^y \bmod p\}\,. \end{aligned}$$

Then, $|S_{00}| = \frac{p-1}{4} - 1$.

Proof of the Lemma II

Proof. First, note that the sets S_{00}, S_{01}, S_{10}, S_{11} are pairwise disjoint. Moreover, for each $x \in \mathbb{Z}_{p-1}$ with $x \neq (p-1)/2$ we have $g^x + 1 \not\equiv 0 \mod p$. Thus, there exists a unique $y \in \mathbb{Z}_{p-1}$ such that $g^x + 1 \equiv g^y \mod p$. Consequently, we obtain

$$|S_{00}| + |S_{01}| + |S_{10}| + |S_{11}| = p - 2\,. \tag{5}$$

Furthermore, we have

$$|S_{11}| = |S_{10}|\,. \tag{6}$$

Condition (6) is true, since the mapping

$$(x, y) \mapsto (-x, y - x)$$

between S_{11} and S_{10} is a bijection.

Proof of the Lemma III

For seeing this, note that $g^{2m+1} + 1 \equiv g^{2n+1} \mod p$ implies

$$g^{2m+1} \cdot g^{-(2m+1)} \equiv 1 \mod p\,.$$

Because of $g^{2m+1} \equiv g^{2n+1} - 1 \mod p$, we get

$$\begin{aligned}
(g^{2n+1} - 1) \cdot g^{-(2m+1)} &\equiv 1 \mod p \\
g^{2n+1} \cdot g^{-(2m+1)} - g^{-(2m+1)} &\equiv 1 \mod p \\
g^{2(n-m)} &\equiv g^{-(2m+1)} + 1 \mod p\,.
\end{aligned}$$

Hence, the mapping defined above is bijective.

Proof of the Lemma IV

Next, we show that $$|S_{10}| = |S_{01}| \,. \tag{7}$$

For seeing this, note that $g^{2m+1} + 1 \equiv g^{2n} \mod p$ implies $-g^{2n} + 1 \equiv -g^{2m+1} \mod p$. The latter congruence and Theorem 2 in turn imply that

$$g^{2n+\frac{p-1}{2}} + 1 \;\equiv\; g^{2m+1+\frac{p-1}{2}} \mod p \,.$$

Therefore, by taking into account that $(p-1)/2$ is even, we see that the mapping

$$(x, y) \mapsto \left(y + \frac{p-1}{2}, x + \frac{p-1}{2}\right)$$

is a bijection between S_{10} and S_{01}.
Moreover, we can also calculate the following:

$$|S_{11}| + |S_{10}| = (p-1)/2 \,. \tag{8}$$

Proof of the Lemma V

Since $S_{11} \cap S_{10} = \emptyset$, we know that $|S_{11}| + |S_{10}| = |S_{11} \cup S_{10}|$. But

$$\begin{aligned} S_{11} \cup S_{10} \quad = \quad & \{(x, y) \mid \ x, y \in \mathbb{Z}_{p-1} \text{ and } x \equiv 1 \mod 2 \\ & \text{and } g^x + 1 \equiv g^y \mod p\}\,, \end{aligned}$$

and therefore,

$$|S_{11} \cup S_{10}| \quad = \quad \frac{p-1}{2}\,.$$

Proof of the Lemma V

Since $S_{11} \cap S_{10} = \emptyset$, we know that $|S_{11}| + |S_{10}| = |S_{11} \cup S_{10}|$. But

$$\begin{aligned} S_{11} \cup S_{10} &= \{(x, y) \mid \; x, y \in \mathbb{Z}_{p-1} \text{ and } x \equiv 1 \mod 2 \\ &\qquad \text{and } g^x + 1 \equiv g^y \mod p\}\,, \end{aligned}$$

and therefore,

$$|S_{11} \cup S_{10}| = \frac{p-1}{2}\,.$$

Finally, putting (6), (7) and (8) together yields

$$|S_{11}| = |S_{10}| = |S_{01}| = \frac{p-1}{4}\,.$$

Thus, by (5) we can conclude $|S_{00}| = \dfrac{p-1}{4} - 1$. This proves Claim 2.

Proof of the Lemma VI

Now, we are ready to show the lemma. Let g be any generator for $\mathbb{Z}_p^*$ and let S_{00} be defined with respect to g as in Claim 2. Furthermore, we define

$$\begin{aligned} R &=_{df} \left\{\gamma \in \mathbb{Z}_p^* \mid \left(\frac{\gamma^2 - a}{p}\right) = 1\right\} \quad \text{and} \\ S &=_{df} \left\{b \in \mathbb{Z}_p^* \mid \left(\frac{b - a}{p}\right) = 1 \text{ and } \left(\frac{b}{p}\right) = 1\right\} . \end{aligned}$$

Claim 3. $|R| = 2|S|$.

Let $b \in S$, then $\left(\frac{b}{p}\right) = 1$. Hence, b is a quadratic residue modulo p. Consequently, $x^2 \equiv b \mod p$ is solvable and there are two different solutions γ_1 and γ_2, i.e.,

$$\gamma_1^2 \equiv b \mod p \quad \text{and} \quad \gamma_2^2 \equiv b \mod p .$$

Proof of the Lemma VII

Therefore, from $\left(\frac{b-a}{p}\right) = 1$ we can immediately conclude that $\left(\frac{\gamma_i^2-a}{p}\right) = 1$ for $i = 1, 2$. But this means that every element from S gives rise to two elements of R. Hence, Claim 3 is shown.

Moreover, since $\left(\frac{a}{p}\right) = 1$ and $p \equiv 1 \mod 4$ by assumption, we know $(p-1)/2$ is even, and we get $\left(\frac{-a}{p}\right) = 1$, too (cf. the case $p \equiv 3 \mod 4$).
By Theorem 1 we have $\mathrm{dlog}_g(-a)$ is even, say $2m = \mathrm{dlog}_g(-a)$. Hence, we arrive at

$$-a \equiv g^{2m} \mod p\,.$$

Proof of the Lemma VIII

Now, for every $b \in S$ we obtain *mutatis mutandis* that there is an n such that $2n = \operatorname{dlog}_g b$ and an r with $2r = \operatorname{dlog}_g(b - a)$. Therefore, it holds

$$b - a \equiv g^{2n} + g^{2m} \equiv g^{2r} \mod p\,; \quad \text{and thus}$$
$$g^{2(n-m)} + 1 \equiv g^{2(r-m)} \mod p\,.$$

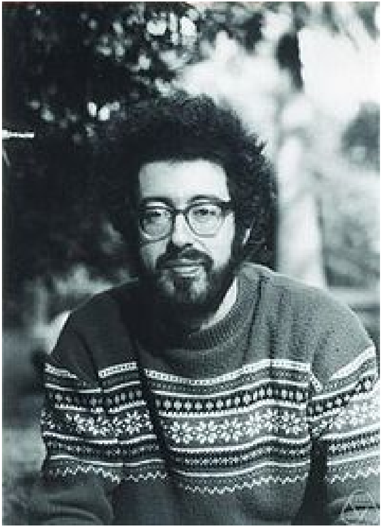
Let $\nu = 2(n - m) \mod (p - 1)$ and $\omega = 2(r - m) \mod (p - 1)$. Then we obviously have $\nu \equiv 0 \mod 2$, $\omega \equiv 0 \mod 2$ and $g^\nu + 1 \equiv g^\omega \mod p$, thus $(\nu, \omega) \in S_{00}$.
Clearly, $b \mapsto (\nu, \omega)$ is an injection from S into S_{00}. Hence, $|S| \leqslant |S_{00}|$ and therefore, by Claim 2, $|S| \leqslant (p - 1)/4 - 1$.
Finally, applying Claim 3 yields $|R| = 2|S| \leqslant (p - 1)/2 - 2$. This proves the lemma. ∎

Thank you!

Adrien-Marie Legendre
(caricature by Julien-Leopold Boilly)

Leonhard Euler

Carl Gustav Jacob **Jacobi**



Robert M. Solovay

Volker Strassen

Carl Friedrich Gauß

Elwyn Berlekamp