Jacobi symbols, primality, and applications

september 2011

1 The group $(\mathbb{Z}/N\mathbb{Z})^*$

We review the structure of the abelian group $(\mathbb{Z}/N\mathbb{Z})^*$. Using Chinese remainder theorem, we can restrict to the case when $N = p^k$ is a prime power. If $k = 1$ the group is cyclic. Assume $k \geq 2$.

The cardinality of $(\mathbb{Z}/p^k\mathbb{Z})^*$ is $p^{k-1}(p-1)$. Since $p-1$ and p^{k-1} are coprime, the group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is the direct product of two subgroups with respective orders $p-1$ and p^{k-1}. One can be more precise.

We have the exact sequence

$$1 \to \mathbf{U}_1 \to (\mathbb{Z}/p^k\mathbb{Z})^* \to \mathbb{F}_p^* \to 1 \tag{1}$$

where $\mathbf{U}_1$ is the subgroup of all $x \bmod p^k$ such that $x \equiv 1 \bmod p$.

Let $\mathbf{V}$ be the group of solutions to the equation $x^{p-1} = 1$. According to Hensel lemma, there are at least $p-1$ such roots, and reduction modulo p is a bijection from $\mathbf{V}$ onto $\mathbb{F}_p^*$. The intersection of $\mathbf{V}$ and $\mathbf{U}_1$ is trivial.

For every $n \geq 1$ let $\mathbf{U}_n \subset (\mathbb{Z}/N\mathbb{Z})^*$ be the subgroup consisting of all residues congruent to 1 modulo p^n. So $\{1\} = \mathbf{U}_k \subset \mathbf{U}_{k-1} \subset \ldots \subset \mathbf{U}_1$.

For every $1 \leq n \leq k-1$, the quotient $\mathbf{U}_n/\mathbf{U}_{n+1}$ is cyclic of order p and $1 + p^n$ is a generator of it. Indeed, the map

$$1 + ap^n \bmod p^{n+1} \mapsto a \bmod p$$

is and isomorphism from $(\mathbf{U}_n/\mathbf{U}_{n+1}, \times)$ onto $(\mathbb{Z}/p\mathbb{Z}, +)$.

Lemma 1 *Let n be an integer such that $1 \leq n \leq k-2$ if $p \geq 3$ and $2 \leq n \leq k-2$ if $p = 2$. Let $x \in \mathbf{U}_n - \mathbf{U}_{n+1}$. Then $x^p \in \mathbf{U}_{n+1} - \mathbf{U}_{n+2}$.*

Indeed $x = 1 + ap^n$ and a is prime to p. If $p \geq 3$ one computes

$$x^p = (1+ap^n)^p = 1+ap^{n+1}+\sum_{2\leq m\leq p-1} \binom{p}{m} a^m p^{nm}+a^p p^{np} \equiv 1+ap^{n+1} \bmod p^{n+2}$$

since $np \geq n+2$.

If $p = 2$ and $n \geq 2$ then

$$x^2 = (1 + a2^n)^2 = 1 + a2^{n+1} + a^2 2^{2n} \equiv 1 + a2^{n+1} \bmod 2^{n+2}$$

since $2n \geq n+2$. $\square$

We deduce that if $p \geq 3$ then $\mathbf{U}_1$ is cyclic of order p^{k-1} and $1+p$ is a generator.

For $p=2$, we only prove that $\mathbf{U}_2$ is cyclic of order 2^{k-2} and 5 is a generator.

If p is odd the group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$.

For $p=2$ one checks that $\mathbf{U}_1 = \{1,-1\} \times \mathbf{U}_2$ so $\mathbb{Z}/2^k\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$.

2 The Legendre symbol

Let p be and odd prime. For every integer x one defines the Legendre symbol $\left(\frac{x}{p}\right)$ as follows :

1. $\left(\frac{x}{p}\right) = 0$ if p divides x,
2. $\left(\frac{x}{p}\right) = 1$ if x is a non-zero square modulo p,
3. $\left(\frac{x}{p}\right) = -1$ if x is not a square modulo p.

The map $x \mapsto \left(\frac{x}{p}\right)$ is a group homomorphism from $\mathbb{F}_p^*$ onto $\{1,-1\}$.

One checks that $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \bmod p$. So we obtain a first method to compute this Legendre symbol.

The famous quadratic reciprocity law states that

Theorem 1 *If p and q are two odd positive distinct primes then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

There are many proofs for this theorem. For example set

$$\Phi_q(x) = 1 + x + \cdots + x^{q-1}$$

and let $A(x) \in \mathbb{F}_p[x]$ be an irreducible factor of $\Phi_q(x)$ modulo p. Set

$$\mathbf{L} = \mathbb{F}_p[x]/A$$

and let $\zeta = x \bmod A(x) \in \mathbf{L}$. This is a q-th root of unity in the field $\mathbf{L}$.

Question 1 *Show that ζ is a primitive q-th root of unity (its multiplicative order is exactly q).*

The so called *Gauss sum*

$$\tau = \sum_{x \in \mathbb{F}_q^*} \left(\frac{x}{q} \right) \zeta^x$$

is an element of the field $\mathbf{L}$.

One can show that $\tau^2 = \left(\frac{-1}{q} \right) q \in \mathbf{L}$. So τ is a square root of $\left(\frac{-1}{q} \right) q$ in the algebraic closure of $\mathbb{F}_p$. This square root is in $\mathbb{F}_p$ if and only if $\tau^p = \tau$. On checks that $\tau^p = \left(\frac{p}{q} \right) \tau$. So $\left(\frac{-1}{q} \right) q$ is a square modulo p if and only if $\left(\frac{p}{q} \right) = 1$. This finishes the proof. □

We shall need also the following theorem

Theorem 2 *For p an odd prime*

$$\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}. \tag{2}$$

Observe that if x is an odd integer then $x = 1 + 2k$ and

$$x^2 = 1 + 4k(k+1) = 1 + 8 \binom{k+1}{2}$$

is congruent to 1 modulo 8. And $k(k+1)/2$ is even if and only if k is congruent to 0 or 3 modulo 4 that is x congruent to 1 or 7 modulo 8.

Now let $A(x) \in \mathbb{F}_p[x]$ be an irreducible factor of $x^4 + 1$ modulo p and set $\zeta = x \bmod A(x)$ the class of x in $\mathbb{F}_p[x]/A$.

Question 2 *Prove that ζ is a primitive 8-th root of 1.*

One checks that $(\zeta + \zeta^{-1})^2 = 2$. So we have a square root of 2 in the algebraic closure of $\mathbb{F}_p$. So 2 is a square if and only if this square root is in $\mathbb{F}_p$ that is $\alpha^p = \alpha$.

But $\alpha^p = \zeta^p + \zeta^{-p}$ where the exponents p only matter modulo 8. If p is congruent to 1 or -1 modulo 8 one deduces that $\alpha^p = \alpha$. If p is congruent to 3 or 5 modulo 8 one checks that $\alpha^p = -\alpha$. This proves formula (2) and the theorem.

3 The Jacobi symbol

Assume $N \geq 3$ is an odd integer and let $N = \prod_i p_i^{e_i}$ its prime decomposition. The Jacobi symbol is defined as a generalization of the Legendre symbol. One sets

$$\left(\frac{x}{N} \right) = \prod_i \left(\frac{x}{p_i} \right)^{e_i}.$$

This symbol only depends on the congruence class of x modulo N. It has many evident multiplicative properties (inherited from the Lengendre symbol). For example $\left(\dfrac{a}{b}\right) = 0$ if and only if a are b not coprime.

The *quadratic reciprocity law* extends to this symbol.

Theorem 3 (Gauss) *Let $M \geq 3$ and $N \geq 3$ two odd coprime integers. One has $\left(\dfrac{-1}{M}\right) = (-1)^{\frac{M-1}{2}}$, $\left(\dfrac{2}{M}\right) = (-1)^{\frac{M^2-1}{8}}$, and*

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\frac{(M-1)(N-1)}{4}}.$$

Thanks to this theorem we can quickly compute the Jacobi symbol by successive Euclidean divisions.

Note that if N is not a prime, the Jacobi symbol does not distinguish quadratic residues. For example if $N = pq$ is the product of two odd primes and if x is prime to N then $\left(\dfrac{x}{N}\right) = 1$ means that either x is a square modulo p and modulo q, or that is not a square modulo p nor modulo q. In the latter case one sometimes says that x is a *false square*.

4 The Solovay-Strassen primality test

Let N be an odd integer. Let $\chi_1 : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ and $\chi_2 : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ be the two group homomorphisms defined by

$$\chi_1 : x \mapsto x^{\frac{N-1}{2}} \bmod N$$

and

$$\chi_2 : x \mapsto \left(\frac{x}{N}\right) \bmod N.$$

We set $\chi_0 = \chi_2/\chi_1$. It is evident that χ_0 is trivial if N is a prime. One has the

Lemma 2 *If N is odd and composite, then there exists an $x \bmod N$ in $(\mathbb{Z}/N\mathbb{Z})^*$ such that $\chi_0(x) \neq 1$.*

Assume first that N is divisible by a non-trivial square : there exists an odd prime p and an integer $k \geq 2$ such that p^k divides exactly N. Set $M = N/p^k$. Let $G \subset (\mathbb{Z}/N\mathbb{Z})^*$ be the subgroup consisting of all residues congruent to 1 modulo Mp. This is a cyclic group of order p^{k-1}. The restriction of the Jacobi symbol to this sub-group is trivial. The restriction of χ_1 is not because $\frac{N-1}{2}$ is prime to p.

Assume now that N is square-free. Let p be an odd prime factor of N and set $M = N/p$. Let x be an integer congruent to 1 modulo M and which is not a square modulo p. Then $\chi_2(x) = -1$ and $\chi_1(x) = 1 \bmod M$. So $\chi_1(x) \neq \chi_2(x)$. $\square$

If N is an odd composite integer then the kernel of χ_0 is a strict subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Its cardinality is $\leq \frac{N-1}{2}$. We have at least one chance over two to find $\chi_0(x) \neq 1$ if x is chosen at random uniformly in $(\mathbb{Z}/N\mathbb{Z})^*$. Since we have polynomial time algorithms to compute χ_1 and χ_2 we obtain a probabilistic primality test :

1. check that N is odd;
2. pick x at random in $(\mathbb{Z}/N\mathbb{Z})^*$ and compute $\chi_1(x)$ and $\chi_2(x)$;
3. if $\chi_1(x) \neq \chi_2(x)$, one knows that N is composite;
4. if $\chi_1(x) = \chi_2(x)$, one cannot conclude ... but one can try again !

If N is odd and composite and if $x \in (\mathbb{Z}/N\mathbb{Z})^*$ is such that $\chi_1(x) = \chi_2(x)$, one says that x is a false witness.

The proportion of false witnesses is at most 1/2.