

Math 104B, Number Theory, Winter 2003.

Lecture 15. Continued Fractions.

Last time:

Definition. If m is odd with prime factorization $m = p_1 \dots p_k$, the the Jacobi symbol $\left(\frac{a}{m}\right)$ is defined by

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right).$$

Note that $\left(\frac{a}{m}\right)$ does not in general determine whether a is a quadratic residue modulo p . Indeed, if $m = p_1^{b_1} \dots p_k^{b_k}$ is the prime factorization then

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{b_1} \dots \left(\frac{a}{p_k}\right)^{b_k} = 1 \Leftrightarrow \sum_{j: \left(\frac{a}{p_j}\right) = -1} b_j \text{ is even.}$$

But a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p_j for every j which holds if and only if $\left(\frac{a}{p_j}\right) = 1$ for every j . Indeed, suppose that a is a quadratic residue modulo p_j for every j . Then by Proposition 9.3.1, a is a quadratic residue modulo $p_j^{b_j}$, so there exists x_j with $x_j^2 \equiv a \pmod{p_j^{b_j}}$. But solving $x \equiv x_j \pmod{p_j^{b_j}}$ using the Chinese Remainder Theorem gives $x^2 \equiv a \pmod{m}$.

For example, take primes 5 and 7 and take a number which is a quadratic non-residue modulo both 5 and 7, for example 3. Then $\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right) \left(\frac{3}{7}\right) = (-1)(-1) = 1$, but 3 is not a quadratic residue modulo 35.

Lemma. If m, n are odd then

(a)
$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right),$$

(b)
$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right),$$

(c)
$$a \equiv b \pmod{m} \quad \Rightarrow \quad \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right),$$

(d)
$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2},$$

$$(e) \quad \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8},$$

$$(f) \quad \left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4},$$

Proof of (d), (e), (f). $m = p_1 \dots p_k$.

Note for p, q prime, we do have

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{(p-1)/2} \equiv p \pmod{4} \\ \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8} \\ \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) &= (-1)^{(p-1)(q-1)/4}. \end{aligned}$$

(d).

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \dots \left(\frac{-1}{p_k}\right) \equiv p_1 \dots p_k \equiv m \equiv (-1)^{(m-1)/2} \pmod{4}.$$

(e). For m odd, set we show that $(-1)^{(m^2-1)/8}$ is multiplicative in m , that is

$$(-1)^{((mn)^2-1)/8} = (-1)^{(m^2-1)/8} (-1)^{(n^2-1)/8}.$$

This is proved by considering all possible values of odd m and n modulo 8. Indeed,

$$(-1)^{(m^2-1)/8} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}.$$

Multiplication modulo 8 gives

$$\begin{array}{ccccc} \times & 1 & -1 & 3 & -3 \\ 1 & 1 & -1 & 3 & -3 \\ -1 & -1 & 1 & -3 & 3 \\ 3 & 3 & -3 & 1 & -1 \\ -3 & -3 & 3 & -1 & 1 \\ & & & 2 & \end{array},$$

For example if m is 1 or -1 modulo 8 and n is 3 or -3 modulo 8, then mn is 3 or -3 modulo 8 and so

$$(-1)^{((mn)^2-1)/8} = -1, \quad (-1)^{(m^2-1)/8}(-1)^{(n^2-1)/8} = -1.$$

Now we have established this multiplicativity property, we have

$$\left(\frac{2}{m}\right) = \left(\frac{2}{p_1}\right) \dots \left(\frac{2}{p_k}\right) = (-1)^{(p_1^2-1)/8} \dots (-1)^{(p_k^2-1)/8} = (-1)^{(m^2-1)/8}.$$

(f). For m and n odd, we will show that $(-1)^{\frac{m-1}{2} \frac{n-1}{2}}$ has a multiplicativity property, indeed,

$$(-1)^{\frac{m-1}{2} \frac{n-1}{2}} = \begin{cases} 1 & n \equiv 1 \pmod{4} \\ (-1)^{\frac{m-1}{2}} & n \equiv -1 \pmod{4}. \end{cases}$$

Since we have already established

$$(-1)^{(m_1 m_2 - 1)/2} = (-1)^{(m_1 - 1)/2} (-1)^{(m_2 - 1)/2},$$

we get

$$(-1)^{\frac{m_1 m_2 - 1}{2} \frac{n-1}{2}} = (-1)^{\frac{m_1 - 1}{2} \frac{n-1}{2}} (-1)^{\frac{m_2 - 1}{2} \frac{n-1}{2}}.$$

Hence

$$\left(\frac{m}{q}\right) \left(\frac{q}{m}\right) = \left(\frac{p_1}{q}\right) \dots \left(\frac{p_k}{q}\right) \left(\frac{q}{p_1}\right) \dots \left(\frac{q}{p_k}\right) = (-1)^{\frac{p_1-1}{2} \frac{q-1}{2}} \dots (-1)^{\frac{p_k-1}{2} \frac{q-1}{2}} = (-1)^{\frac{m-1}{2} \frac{q-1}{2}},$$

which proves the result when n (or m) is prime. Now we repeat the argument with n odd,

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \left(\frac{p_1}{n}\right) \dots \left(\frac{p_k}{n}\right) \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right) = (-1)^{\frac{p_1-1}{2} \frac{n-1}{2}} \dots (-1)^{\frac{p_k-1}{2} \frac{n-1}{2}} = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}.$$

This completes the proof.

Continued Fractions. We did Example like 11.1.1 to introduce continued fractions.