7. Quadratic Reciprocity

Def'n For $n \in \mathbb{N}$, the **Euler φ-function** is defined by
$$\varphi(n) = \#\{1 \le m \le n;\ (m,n) = 1\}.$$

Theorem 32 (Euler's Theorem): Let $a \in \mathbb{N}$ with $(a,n) = 1$. Then
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof: Let $c_1, c_2, \dots, c_{\varphi(n)}$ be a reduced residue system mod n. Since $(a,n) = 1$, then $ac_1, ac_2, \dots, ac_{\varphi(n)}$ is also a reduced residue system mod n. Thus
$$\begin{aligned} & c_1 \cdots c_{\varphi(n)} \equiv (ac_1) \cdots (ac_{\varphi(n)}) \pmod{n} \\ \Rightarrow\ & c_1 \cdots c_{\varphi(n)} \equiv a^{\varphi(n)} (c_1 \cdots c_{\varphi(n)}) \pmod{n} \\ \Rightarrow\ & a^{\varphi(n)} \equiv 1 \pmod{n}. \end{aligned}$$
∎

Corollary 33 (Fermat's Little Theorem): Let p be a prime. Then for any $a \in \mathbb{Z}$ with $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 34 (Wilson's Theorem): Let p be a prime. Then
$$(p-1)! \equiv -1 \pmod{p}.$$

Proof: Consider the polynomial $x^{p-1} - 1$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. By Corollary 33, $1, 2, \dots, p-1$ are its roots. Thus in $(\mathbb{Z}/p\mathbb{Z})[x]$, we have
$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)).$$
Consider the constant coefficients on both sides, we see that
$$-1 \equiv (-1)(-2)\cdots(-(p-1)) \equiv (-1)^{p-1}(p-1)! \pmod{p}.$$
If $p = 2$, the result holds since $-1 = 1$. Otherwise, p is odd, so
$$-1 \equiv (p-1)! \pmod{p}.$$
∎

Def'n Let p be a prime and let $a \in \mathbb{Z}$ with $(a,p) = 1$. We define the **Legendre symbol** $\left(\frac{a}{p}\right)$ by the rule
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise.} \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$, we say a is a <u>quadratic residue mod p</u>, otherwise a is a <u>quadratic nonresidue mod p</u>.

Theorem 35 (Euler's Criterion): Let p be an odd prime and let $a \in \mathbb{Z}$ with $(a,p) = 1$. Then

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

Proof: The congruence $x^2 \equiv a \pmod{p}$ has at most two solutions mod p. Two cases:

(1) Suppose that there is a solution, say b. Thus $\left(\frac{a}{p}\right) = 1$. Since $b^2 \equiv a \pmod{p}$,

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Thus

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

(2) Suppose that $x^2 \equiv a \pmod{p}$ has no solution. Then $\left(\frac{a}{p}\right) = -1$. Since $(a,p) = 1$, for each fixed $r \in (\mathbb{Z}/p\mathbb{Z})^*$ there exists a unique $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $rs \equiv a \pmod{p}$. Since $x^2 \equiv a \pmod{p}$ has no solution, we see that $r \neq s$. Split elements in $(\mathbb{Z}/p\mathbb{Z})^*$ into $\frac{p-1}{2}$ pairs (r,s) with $r \neq s$ and $rs \equiv a \pmod{p}$. Thus

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

By Theorem 34, we have $(p-1)! \equiv -1 \pmod{p}$. It follows that

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

Theorem 36: Let p be an odd prime and let $a, b \in \mathbb{Z}$. Then

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Also,

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

Here for $a \in \mathbb{Z}$, $p \mid a$, we extend the definition of the Legendre symbol and define $\left(\frac{a}{p}\right) = 0$.

Proof: The statement holds if $p \mid ab$ (equivalent to $p \mid a$ or $p \mid b$). Thus we may assume $p \nmid a$ and $p \nmid b$.
By Euler's criterion,

2015 10 26

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are in $\{-1, 1\}$ and p is an odd prime, we see that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

By Euler's criterion,

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

Since $\left(\frac{-1}{p}\right) \in \{-1, 1\}$ and p is an odd prime, it follows that

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

■

Theorem 37 (Gauss' Lemma): Let p be an odd prime and let $a \in \mathbb{Z}$ with $(a, p) = 1$. Let μ be the number of integers from $\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\}$ whose residues mod p of least absolute value (ie. residues taking value between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$) are negative. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Ex. Let $p = 5$ and $a = 2$. Consider $\{2, 4\}$. Then their residues mod 5 of least absolute value are 2 and -1. Thus $\mu = 1$ and

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

Proof: We first replace the integers $a, 2a, \dots, (\frac{p-1}{2})a$ by their residues of least absolute value. We denote the negative ones by $-s_1, -s_2, \dots, -s_\mu$ and the positive ones by $r_1, r_2, \dots, r_{\frac{p-1}{2}-\mu}$. Since $1 \le r_i, s_j \le \frac{p-1}{2}$, no two r_i's are equal and no two s_j's are equal.

Claim: $r_i \neq s_j$ for any i, j.

Verification: Note that if $m_1 a \equiv r_i \pmod p$ and $m_2 a \equiv -s_j \pmod p$ with $r_i = s_j$ then $(m_1+m_2)a \equiv 0 \pmod p$. Since $(a,p) = 1$, it follows that $p \mid (m_1+m_2)$, which is not possible since $1 \le m_1, m_2 \le \frac{p-1}{2}$. Thus the claim holds. □

Since no two r_i's are equal, no two s_j's are equal, and $r_i \neq r_j$ for any i, j, we see that $s_1, \dots, s_\mu, r_1, \dots, r_{\frac{p-1}{2}-\mu}$ is a rearrangement of $1, 2, \dots, \frac{p-1}{2}$. Thus

$$a(2a)\cdots\left(\left(\tfrac{p-1}{2}\right)a\right) \equiv 1\cdot 2\cdots\left(\tfrac{p-1}{2}\right)(-1)^\mu \pmod p.$$

It follows that

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod p.$$

By Euler's criterion,

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

Since $(-1)^\mu$ and $\left(\frac{a}{p}\right)$ are in $\{-1, 1\}$ and p is an odd prime, we see that

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$ ■

Corollary 38: If p is an odd prime, then

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

Proof: Consider the set $\{2, 4, \dots, (\frac{p-1}{2})2\}$. Note that $2r \le \frac{p-1}{2}$ if and only if $r \le \frac{p-1}{4}$. Thus the number of integers on the set whose residues of least absolute value are negative is equal to

$$\mu = \left(\frac{p-1}{2}\right) - \left\lfloor \frac{p-1}{4} \right\rfloor.$$

Note that if $p = 8k+1$, then

$$\mu = 4k - \left\lfloor \frac{8k}{4} \right\rfloor = 4k - 2k \equiv 0 \pmod 2.$$

If $p = 8k+3$, then

$$\mu = (4k+1) - 2k = 2k+1 \equiv 1 \pmod 2.$$

If $p = 8k+5$, then

$$\mu = (4k+2) - (2k+1) = 2k+1 \equiv 1 \pmod 2.$$

If $p = 8k+7$, then

$$\mu = (4k+3) - (2k+1) = 2k+2 \equiv 0 \pmod 2.$$

By Gauss' Lemma,

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

Thus 2 is a quadratic residue mod p if $p \equiv \pm 1 \pmod 8$ and 2 is a quadratic non-residue mod p if $p \equiv \pm 3 \pmod 8$. Note that if $p \equiv \pm 1 \pmod 8$ then $\frac{p^2-1}{8}$ is even. If $p \equiv \pm 3 \pmod 8$, then $\frac{p^2-1}{8}$ is odd. Thus

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

Theorem 39 (Law of Quadratic Reciprocity): If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Ex. What is $\left(\frac{13}{17}\right)$? By the law of quadratic reciprocity,

$$\left(\frac{13}{17}\right) = (-1)^{\left(\frac{17-1}{2}\right)\left(\frac{13-1}{2}\right)} \left(\frac{17}{13}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1.$$

Ex. Claim: 5 is a quadratic residue for all primes of the form $10k \pm 1$, and a quadratic non-residue for all primes of the form $10k \pm 3$.

good final exam question

Proof (of claim): Note that

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

Note that ± 1 are quadratic residues mod 5, and ± 3 are quadratic non-residues mod 5. Thus $\left(\frac{p}{5}\right)=1$ if $p = 10k \pm 1$ and $\left(\frac{p}{5}\right)=-1$ if $p = 10k \pm 3$. □

2015 10 28

Proof (of theorem 39): By Gauss' lemma,

$$\left(\frac{p}{q}\right) = (-1)^{\mu} \quad \text{and} \quad \left(\frac{q}{p}\right) = (-1)^{\nu},$$

where μ is the number of integers from $\{p, 2p, \ldots, (\frac{q-1}{2})p\}$ whose residue mod q of least absolute value is negative and ν is the number of integers from $\{q, 2q, \ldots, (\frac{p-1}{2})q\}$ whose residue mod p of least absolute value is negative. Thus to prove the theorem, it suffices to show

$$\mu + \nu \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod 2.$$

Claim: For $x \in \mathbb{Z}$ with $1 \le x \le \frac{q-1}{2}$, there exists a unique $y \in \mathbb{Z}$ such that $-\frac{q}{2} < xp - qy < \frac{q}{2}$. Furthermore, $y \ge 0$.
(Note: $xp - yq$ is the residue mod q of the least absolute value of xp.)
Verification: Note that

$$-\frac{q}{2} < xp - yq < \frac{q}{2} \implies \frac{-xp}{q} - \frac{1}{2} < -y < \frac{-xp}{q} + \frac{1}{2}. \qquad \text{——} \star$$

Thus y is uniquely determined. Also, we note that if $y<0$, then $xp - yq \ge q$. Since $xp - yq \in (-\frac{q}{2}, \frac{q}{2})$ we see that $y \ge 0$. □
Note that if $y=0$, there is no contribution from $xp - yq$ to μ since $xp > 0$.
Also, if $x = \frac{q-1}{2}$, then from $\star$,

$$y < \frac{xp}{q} + \frac{1}{2} = \frac{(\frac{q-1}{2})p}{q} + \frac{1}{2} = \frac{p}{2}\left(\frac{q-1}{q}\right) + \frac{1}{2} < \frac{p+1}{2}.$$

Since $y \in \mathbb{Z}$, $y \le \frac{p-1}{2}$. Thus the number μ corresponds to the number of combinations of x and y from the sequences

(A) $1, 2, \ldots, \frac{q-1}{2}$
(B) $1, 2, \ldots, \frac{p-1}{2}$

respectively such that $-\frac{q}{2} < xp - yq < 0$, or equivalently, such that $0 < yq - xp < \frac{q}{2}$. Similarly, ν is the number of combinations of x and y from the sequences (A) and (B) respectively, for which $-\frac{p}{2} < yq - xp < 0$. For any

other pairs (x,y) with x from (A) and y from (B), either $yq-xp<-\frac{p}{2}$ or $yq-xp>\frac{q}{2}$. Let ρ be the number of pairs (x,y) for which $yq-xp<-\frac{p}{2}$ and let λ be the number of pairs (x,y) for which $yq-xp>\frac{q}{2}$. Then

$$\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right)=\mu+\nu+\rho+\lambda.$$

As x and y run through (A) and (B) respectively,

$$x'=\frac{q+1}{2}-x \quad \text{and} \quad y'=\frac{p+1}{2}-y$$

run through (A) and (B) respectively, but in reverse order. Note that $yq-xp<-\frac{p}{2}$ if and only if

$$y'q-x'p=\left(\frac{p+1}{2}-y\right)q-\left(\frac{q+1}{2}-x\right)p$$

$$=\frac{q-p}{2}-(yq-xp)>\frac{q}{2}.$$

Furthermore, $yq-xp>\frac{q}{2}$ if and only if

$$y'q-x'p=\frac{q-p}{2}-(yq-xp)<-\frac{p}{2}.$$

Then $\rho=\lambda$. It follows that

$$\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right)=\mu+\nu+\rho+\lambda\equiv\mu+\nu \pmod 2. \qquad \blacksquare$$

Ex. Claim: The equation $x^4-17y^4=2w^2$ has no integer solutions.
Suppose that there exist $x,y,w\in\mathbb{Z}$ such that $x^4-17y^4=2w^2$.
Without loss of generality, we can assume x and y are coprime.
Thus x and w are coprime. Note that if p is an odd prime which divides w, since $x^4\equiv 17y^4 \pmod p$, ie. $17\equiv(x^2y^{-2})^2 \pmod p$, we have $\left(\frac{17}{p}\right)=1$. By the law of quadratic reciprocity,

$$\left(\frac{p}{17}\right)=(-1)^{\frac{17-1}{2}\frac{p-1}{2}}=1.$$

Thus an odd prime dividing w is a quadratic residue mod 17.
Also, by corollary 38,

$$\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=1.$$

By the above arguments, we see that any prime dividing w is a quadratic residue mod 17. Thus $w = t^2 \pmod{17}$ for some $t \in \mathbb{Z}$. Note that $17 \nmid w$, and thus $17 \nmid t$. Since $x^4 - 17y^4 = 2w^2$, it follows that $x^4 \equiv 2t^4 \pmod{17}$. Thus $2 \equiv x^4 t^{-4} \pmod{17}$, ie. there exists $r \in \mathbb{Z}$ such that $2 \equiv r^4 \pmod{17}$, which is a contradiction.

Ex. Is the congruence $3x^2 + 7x - 42 \equiv 0 \pmod{391}$ solvable?
By multiplying both sides by 12, we get

$$36x^2 + 84x - 516 \equiv 0 \pmod{391}$$
$$\Rightarrow (6x+7)^2 \equiv 565 \pmod{391}.$$

Thus it suffices to consider $y^2 \equiv 174 \pmod{391}$. Note that $391 = 17 \cdot 23$. We see that $y^2 \equiv 174 \pmod{17}$ is equivalent to $y^2 \equiv 4 \pmod{17}$, which has a solution. Also, $y^2 \equiv 174 \pmod{23}$ is equivalent to $y^2 \equiv 13 \pmod{23}$. By the law of quadratic reciprocity,

$$\left(\frac{13}{23}\right) = (-1)^{\frac{13-1}{2}\frac{23-1}{2}} \left(\frac{23}{13}\right) = \left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{5}\right)\left(\frac{5}{13}\right).$$

Since both 2 and 5 are quadratic non-residues mod 13, we have

$$\left(\frac{13}{23}\right) = (-1)(-1) = 1.$$

Thus $y^2 \equiv 13 \pmod{23}$ has a solution. Since both $y^2 \equiv 4 \pmod{17}$ and $y^2 \equiv 13 \pmod{23}$ have a solution, by the Chinese Remainder Theorem, $y^2 \equiv 174 \pmod{391}$ has a solution.

Ex What is $\left(\frac{713}{1009}\right)$?
Note that $713 = 23 \cdot 31$. Then by theorem 36,

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$$

By the law of quadratic reciprocity,

$$\left(\frac{23}{1009}\right) = (-1)^{\frac{23-1}{2}\frac{1009-1}{2}} \left(\frac{1009}{23}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right).$$

Since 4 is a square,

$$\left(\frac{20}{23}\right) = \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right).$$

Also, by the law of quadratic reciprocity,

$$\left(\frac{5}{23}\right) = (-1)^{\frac{5-1}{2}\frac{23-1}{2}}\left(\frac{23}{5}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

It follows that

$$\left(\frac{23}{1009}\right) = \left(\frac{20}{23}\right) = \left(\frac{5}{23}\right) = -1.$$

Similarly (exercise), we have

$$\left(\frac{31}{1009}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right).$$

By corollary 38, we have $\left(\frac{2}{17}\right)=1$. Also, by the law of quadratic reciprocity,

$$\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Thus $\left(\frac{31}{1009}\right) = -1$. It follows that

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right) = (-1)(-1) = 1.$$

Remark: In the above calculation, we are given the fact that $713 = 23 \cdot 31$. However, it is not always easy to find the prime factorization of an integer a. However, it is possible to evaluate $\left(\frac{a}{p}\right)$ without knowing the prime factorization of a.
The idea is to 'flip' the Legendre symbol to $\left(\frac{p}{a}\right)$ even when a is not a prime.

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ be odd. If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, we define the Jacobi symbol

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Theorem 40 (Generalized Law of Quadratic Reciprocity): Let $a, b \in \mathbb{N}$ be odd. We have

(1)
$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \pmod 4 \\ -1 & \text{if } b \equiv 3 \pmod 4 \end{cases}$$

(2) $$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

(3) $$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv 3 \pmod 4 \end{cases}$$

Proof: Exercise ∎

Ex We now compute $\left(\frac{713}{1009}\right)$.
By the generalized law of quadratic reciprocity, since $713 \equiv 1 \pmod 4$ $713 \equiv 1 \pmod 8$, we have

$$\left(\frac{713}{1009}\right) = \left(\frac{1009}{713}\right) = \left(\frac{296}{713}\right) = \left(\frac{2^3 \cdot 37}{713}\right) = \left(\frac{37}{713}\right).$$

Now since $37 \equiv 1 \pmod 4$ and $37 \equiv 5 \pmod 8$, we have

$$\left(\frac{37}{713}\right) = \left(\frac{713}{37}\right) = \left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right).$$

Since $5 \equiv 1 \pmod 4$ we have

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$