New York Journal of Mathematics

New York J. Math. **16** (2010) 387–398.

Primes, permutations and primitive roots

Joseph Lewittes and **Victor Kolyvagin**

Abstract. Let p be a prime greater than 3, $X = \{1, 2, \ldots, p-1\}$ and R the set of primitive roots mod p contained in X. To each $g \in R$ associate the permutation σ_g of X defined by $\sigma_g(x) = y$ where y is the unique member of X satisfying $y \equiv g^x \pmod{p}$. Let $\Sigma_R = \{\sigma_g | g \in R\}$. We analyze the parity of the permutations in Σ_R. If $p \equiv 1 \pmod 4$ half the permutations are even and half are odd. If $p \equiv 3 \pmod 4$ they are either all even or all odd; set $\epsilon(p) = 1$ in the even case, $\epsilon(p) = -1$ in the odd case. Numerical evidence suggests the conjecture that $\epsilon(p) \equiv h(-p) \pmod 4$, where $h(-p)$ is the class number of the quadratic field $Q(\sqrt{-p})$. The conjecture is shown to be true, and furthermore $\epsilon(p) \equiv -(\frac{p-1}{2})! \pmod p$. We also study a larger class of permutations of degree $p-1$ which generalize the Σ_R.

Contents

1. Introduction

Fix an odd prime p and let $X = \{1, 2, \ldots, p-1\}$. X will play a dual role, as a reduced system of residues mod p ($0 \bmod p$ has no representative in X) and also as a complete set of residues mod $p-1$. Let R denote the set of primitive roots mod p contained in X. With $g \in R$ we associate the permutation σ_g of X defined by $\sigma_g(x) \equiv g^x \pmod p$. More precisely, $\sigma_g(x) = y$, the unique element of X satisfying $y \equiv g^x \pmod p$. For example, if $p = 7$, $R = \{3, 5\}$, and, in cycle notation, $\sigma_3 = (1\ 3\ 6)(2)(4)(5)$, $\sigma_5 = (1\ 5\ 3\ 6)(2\ 4)$. Note that σ_3 has 3 fixed points $x = 2, 4, 5$ which satisfy $3^x \equiv x \pmod 7$. The permutations σ_g were, apparently, first studied due to a question of Brizolis who asked whether for each p there exist g, x satisfying $\sigma_g(x) = x$, i.e., $g^x \equiv x \pmod p$. The question has been answered affirmatively using methods of analytic number theory and computer searches. A reference for the literature on this topic is in Guy [2, Problem F9 Primitive Roots, p.

Received May 21, 2010.

2000 *Mathematics Subject Classification.* 11A07, 11R29, 20B35.

Key words and phrases. permutation, prime, primitive root, class number.

ISSN 1076-9803/2010

377]. Our interest here is not on fixed points but on the parity of the permutations, are they even or odd. Note that the inverse of the permutation σ_g is just the classical index with respect to g, or, in modern terminology, the discrete logarithm $\log_g$ in the cyclic group of residue classes mod p prime to p. We do not enter into computational aspects of the discrete logarithm.

Some notation. For a permutation σ, $s(\sigma)$ is the sign of σ, which is 1 or -1 according as σ is even or odd. $|A|$ denotes the number of elements of the finite set A. For integers a and b, (a, b) denotes the greatest common divisor of a and b, but in other contexts (a, b) also denotes a transposition interchanging a and b. U is the set of units mod $p-1$ contained in X; thus $U = \{x \in X | (x, p-1) = 1\}$. x, y denote elements of X and u an element of U. For a fixed $g \in R$, the map $U \to R$ by $u \to g^u \pmod p$ is a bijection and $|R| = |U| = \phi(p-1)$, ϕ being Euler's function. Let $\Sigma_R = \{\sigma_g | g \in R\}$; clearly $|\Sigma_R| = |R|$. Σ_R is a subset of S_{p-1}, the symmetric group of degree $p-1$. Are the permutations in Σ_R even or odd? The answer is somewhat unexpected.

Theorem 1.
If $p \equiv 1 \pmod 4$ half the permutations in Σ_R are even and half are odd.
If $p \equiv 3 \pmod 4$ all permutations in Σ_R have the same sign — either all are odd or all are even.

Considering the first few primes we have:

$$\begin{array}{lll} p = 3, & R = \{2\}, & \sigma_2 = (1\ 2) \text{ odd.} \\ p = 5, & R = \{2, 3\}, & \sigma_2 = (1\ 2\ 4)(3) \text{ even;} \\ & & \sigma_3 = (1\ 3\ 2\ 4) \text{ odd.} \end{array}$$

We saw above that $p = 7$ has all even.

For $p \equiv 3 \pmod 4$ we define $\epsilon(p) = 1$ or -1 according as the permutations in Σ_R are all even or all odd. $\epsilon(p)$ seems to be unpredictable. Trying to relate $\epsilon(p)$ with some other function of $p \equiv 3 \pmod 4$ led us to compare it with $h(-p)$, the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ with discriminant $-p$. See [1, p. 346]. It is known that $h(-p)$ is always a positive odd integer. See Table 1 for some calculations.

Up to 47 the permutations were analyzed by hand; beyond this a computer became useful, in fact necessary. The computations in this paper were done using Maple 8. From Table 1, $\epsilon = 1$ and $\epsilon = -1$ appear to be running neck and neck and this behavior persists. Table 2 shows for each value of N the number of primes $\equiv 3 \pmod 4$ up to N having $\epsilon = 1$ and the number having $\epsilon = -1$.

The table shows that up to $p = 199$, $\epsilon(p) \equiv h(-p) \pmod 4$, except for $p = 3$ which is exceptional (the field $\mathbb{Q}(\sqrt{-3})$ contains the 6^{th} roots of unity while all the other fields contain only ± 1). We have checked this for p up to several thousand using the class number tables of Tomita [4]. This leads

TABLE 1. Some values of $\epsilon(p)$ and $h(-p)$

$p \equiv 3 \pmod 4$	$\epsilon(p)$	$h(-p)$	$p \equiv 3 \pmod 4$	$\epsilon(p)$	$h(-p)$
3	-1	1	83	-1	3
7	1	1	103	1	5
11	1	1	107	-1	3
19	1	1	127	1	5
23	-1	3	131	1	5
31	-1	3	139	-1	3
43	1	1	151	-1	7
47	1	5	163	1	1
59	-1	3	167	-1	11
67	1	1	179	1	5
71	-1	7	191	1	13
79	1	5	199	1	9

TABLE 2.

N	$\#(\epsilon = 1)$	$\#(\epsilon = -1)$
200	14	10
1000	44	43
2000	73	82
5000	165	174
10000	309	310

to the empirical conjecture that $\epsilon(p) \equiv h(-p) \pmod 4$ is true; or simply stated, if $p \equiv 3 \pmod 4$ and g is a primitive root mod p then

$$s(\sigma_g) \equiv h(-p) \pmod 4. \tag{1}$$

Theorem 3, below, is our main result and in the remarks following it we show how (1) is a consequence.

Theorem 1 follows from a more general result. We move temporarily from the setting of p, X to a positive integer, m, $A = \mathbf{Z}/(m)$, $U = A^{\times}$, the group of units consisting of the congruence classes mod m relatively prime to m, $|U| = \phi(m)$. For $u \in U$, $\theta_u : A \to A$ is multiplication by u; $\theta_u(x) \equiv ux \pmod m$. Since $\theta_u\theta_v = \theta_{uv}$, $\theta_u^{-1} = \theta_{u^{-1}}$, where u^{-1} is the inverse of $u \pmod m$, each θ_u is a permutation of A. $T = \{\theta_u \mid u \in U\}$ is an abelian group of permutations of A, isomorphic to U and can be thought of as a subgroup of S_m, the symmetric group of degree m. T being a group either all permutations in it are even or half are even and half odd. We will say simply T is even in the former case and even-odd in the latter. Note that as soon as a single θ_u is shown to be odd then T is even-odd.

Theorem 2. *The parity of T depends on m* mod 4:

If $m \equiv 0 \pmod 4$, T is even-odd.

If $m \equiv 1 \pmod 4$, T *is even-odd unless* m *is a square in which case* T *is even.*

If $m \equiv 2 \pmod 4$, T *is even.*

If $m \equiv 3 \pmod 4$, T *is even-odd.*

The proof will be given in the next section. Here we only show how Theorem 1 follows from Theorem 2.

Fix the odd prime p and a primitive root g. Every $h \in R$ is $h \equiv g^u \pmod p$ for a unique unit u, so for $x \in X$, $\sigma_h(x) \equiv h^x \equiv g^{ux} \equiv \sigma_g(ux) \pmod p = \sigma_g\theta_u(x)$. Thus $\sigma_h = \sigma_g\theta_u$ and $\Sigma_R = \sigma_g T$ is a coset of T in S_{p-1}. Now apply Theorem 2 with $m = p-1$ which shows T is even-odd when $p \equiv 1 \pmod 4$ and is even when $p \equiv 3 \pmod 4$. Thus Σ_R is even-odd when $p \equiv 1 \pmod 4$ but $\Sigma_R = \sigma_g T$ shows that when $p \equiv 3 \pmod 4$ all $\sigma_h \in \Sigma$ have the same sign.

Theorem 3. *Let* p *be a prime greater than* 3 *and* g *a primitive root* mod p.

If $p \equiv 3 \pmod 4$, *then*

$$s(\sigma_g) \equiv -\left(\frac{p-1}{2}\right)! \pmod p. \tag{2}$$

If $p \equiv 1 \pmod 4$, *then*

$$s(\sigma_g) \equiv -\left(\frac{p-1}{2}\right)! \cdot g^{\frac{p-1}{4}} \pmod p. \tag{3}$$

This also will be proven in the next section.

Remark 1. (1) is a consequence of (2). To see this we cite a theorem of Mordell [3] which states that for $p \equiv 3 \pmod 4$, $\left(\frac{p-1}{2}\right)! \equiv (-1)^a \pmod p$ where $a \equiv \frac{1}{2}(1 + h(-p)) \pmod 2$. (The proof uses Dirichlet's class number formula. See the references in [3], as well as [1, p. 346], cited earlier.) Thus (2) shows that $s(\sigma_g) \equiv (-1)^{a+1} \pmod p$ or, setting $s(\sigma_g) = (-1)^b$, $(-1)^b \equiv (-1)^{a+1} \pmod p$ which implies $(-1)^b = (-1)^{a+1}$ or $b \equiv a+1 \equiv \frac{1}{2}(1 + h(-p)) + 1 \pmod 2$. Hence $2b \equiv h(-p) + 3 \pmod 4$. If b is even, $s(\sigma_g) = 1$ and $0 \equiv 2b \equiv h(-p) + 3 \pmod 4$ show $h(-p) \equiv 1 \equiv s(\sigma_g) \pmod 4$, while if b is odd, $s(\sigma_g) = -1$ and $2 \equiv 2b \equiv h(-p) + 3 \pmod 4$ show $h(-p) \equiv -1 \equiv s(\sigma_g) \pmod 4$.

Remark 2. Here we only point out that Theorem 1 also follows from Theorem 3, so the reader may skip Theorem 2, if so desired. Indeed, if $p \equiv 3 \pmod 4$ and g, $k \in R$ then (2) shows $s(\sigma_k) \equiv s(\sigma_g) \pmod p$, as they are both congruent to $-\left(\frac{p-1}{2}\right)! \pmod p$. But $-1 \not\equiv 1 \pmod p$ so we are forced to conclude that $s(\sigma_k) = s(\sigma_g)$, hence all permutations in Σ_R have the same sign. Now assume $p \equiv 1 \pmod 4$ and fix $g \in R$. Since $\left(g^{\frac{p-1}{4}}\right)^2 \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p$, $g^{\frac{p-1}{4}}$ is a root of the congruence $X^2 + 1 \equiv 0 \pmod p$ and the other root $-g^{\frac{p-1}{4}} \equiv g^{\frac{p-1}{2}} g^{\frac{p-1}{4}} \equiv g^{3\frac{p-1}{4}} \pmod p$. Every unit $u \in U$ is relatively prime to $p-1$, hence odd, so $u \equiv 1$ or $3 \pmod 4$. For $i = 1, 3$ let

$U_i = \{u \mid u \equiv i \pmod 4\}$. Then $u \to v = p-1-u$ is a bijection of U_1 onto U_3 and so $|U_1| = |U_3|$. If $u \in U_1$, $u\left(\frac{p-1}{4}\right) \equiv \left(\frac{p-1}{4}\right) \pmod{p-1}$. Thus if $k \equiv g^u \pmod p$ with $u \in U_1$, then $k^{\frac{p-1}{4}} \equiv g^{u\frac{p-1}{4}} \equiv g^{\frac{p-1}{4}} \pmod p$, so by (3) we have $s(\sigma_k) \equiv -\left(\frac{p-1}{2}\right) \cdot k^{\frac{p-1}{4}} \equiv -\left(\frac{p-1}{2}\right)! \cdot g^{\frac{p-1}{4}} \equiv s(\sigma_g) \pmod p$ which implies $s(\sigma_k) = s(\sigma_g)$ in this case. Similarly, if $u \in U_3$ and $h \in R$ is $h \equiv g^u \pmod p$, then $u\left(\frac{p-1}{4}\right) \equiv 3\left(\frac{p-1}{4}\right) \pmod{p-1}$ and so $h^{\frac{p-1}{4}} \equiv g^{u\frac{p-1}{4}} \equiv g^{3\frac{p-1}{4}} \equiv -g^{\frac{p-1}{4}} \pmod p$. Then (3) shows $s(\sigma_h) \equiv -s(\sigma_g) \pmod p$, hence $s(\sigma_h) = -s(\sigma_g)$ and so Σ_R is even-odd when $p \equiv 1 \pmod 4$.

2. Proofs

Proof of Theorem 2.

The easiest case is $m \equiv 0 \pmod 4$. Take $u \equiv -1 \pmod m$, $\theta_u(x) \equiv -x \pmod m$. θ_u is an involution on A so its cycle structure consists of 1-cycles (fixed points) and 2-cycles (transpositions). $\theta_u(x) \equiv x \pmod m$ iff $2x \equiv 0 \pmod m$ or $x \equiv \frac{m}{2} \pmod m$, $x \equiv m \pmod m$. Besides these two fixed points the remaining $m-2$ elements of A break up into a product of $\frac{m-2}{2}$ transpositions of the form $(x, m-x)$, $x = 1, 2, \ldots, \frac{m-2}{2}$. Since $\frac{m-2}{2}$ is odd θ_u is an odd permutation and T is even-odd.

Now let m be arbitrary, even or odd, and consider a $\theta_u \in T$. We have to decompose it into cycles. For every divisor $d|m$ let $A(d) = \{x \bmod m | (x,m) = d\}$; A is the disjoint union of all the sets $A(d)$. Note that (x,m) depends only on $x \bmod m$. $(x,m) = d$ iff $(\frac{x}{d}, \frac{m}{d}) = 1$ so $|A(d)| = \phi(\frac{m}{d})$. If $u \in U = A(1)$, $x \in A(d)$ then also $ux \in A(d)$ since $(ux, m) = (x, m)$. The cycle of θ_u containing x is $(x\ ux\ u^2x\ \ldots\ u^{e-1}x)$ where e is the smallest positive integer such that $u^e x \equiv x \pmod m$. This last congruence is equivalent to $\frac{x}{d}(u^e - 1) \equiv 0 \pmod{\frac{m}{d}}$ and since $(\frac{x}{d}, \frac{m}{d}) = 1$ it is equivalent to $u^e \equiv 1 \pmod{\frac{m}{d}}$; which does not depend on x. Thus the $\phi(\frac{m}{d})$ elements of $A(d)$ break up into cycles under θ_u, all having the same length $e = e(u, \frac{m}{d})$, the order of $u \bmod \frac{m}{d}$. So the number of cycles of θ_u on $A(d)$ is

$$c(u,d) = \frac{\phi(\frac{m}{d})}{e(u, \frac{m}{d})}\ . \tag{4}$$

Now assume $m \equiv 2 \pmod 4$. Write $m = 2t$, t odd. The divisors $d|m$ are $d = \delta$, $d = 2\delta$ where $\delta|t$. For $u \in U$ we claim $e = e(u, \frac{m}{\delta})$ and $e' = e(u, \frac{m}{2\delta})$ are equal. For clearly $e' \le e$. But since m is even $u \equiv 1 \pmod 2$, so $u^{e'} \equiv 1 \pmod 2$ and $u^{e'} \equiv 1 \pmod{\frac{m}{2\delta}}$ imply $u^{e'} \equiv 1 \pmod{2 \cdot \frac{m}{2\delta} = \frac{m}{\delta}}$. Thus $e \le e'$, which proves the claim. Also $\phi(\frac{m}{\delta}) = \phi(\frac{t}{\delta})$ and $\phi(\frac{m}{2\delta}) = \phi(\frac{t}{\delta})$ so that (4) shows $c(u,\delta) = c(u, 2\delta)$. Thus for each $\delta|t$, $A(\delta)$ with $A(2\delta)$ provide a total of $2c(u,\delta)$ cycles all having the same length $e(u, \frac{m}{\delta})$. These $2c(u,\delta)$ cycles contribute a $+1$ to sign θ_u. But as δ ranges over the divisors of t this accounts for all the cycles, showing sign $\theta_u = 1$ for every $\theta_u \in T$ and T is even.

Now let m be odd. Let $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ be the prime factorization of m. Since each p_i is odd there is a primitive root $g_i \mod p_i^{k_i}$. For $i = 1$, $2, \dots, r$ define u_i mod m by the congruence $u_i \equiv g_i \pmod{p_i^{k_i}}$ and $u_i \equiv 1 \pmod{m/p_i^{k_i}}$. By the Chinese Remainder Theorem the u_i generate the group of units U in A and then the θ_{u_i} generate T. To focus on a particular one, say θ_{u_1}, we set $q = p_1$, $k = k_1$, $t = p_2^{k_2} \dots p_r^{k_r}$ (if $r = 1$, $t = 1$). Now $m = q^k t$ and every $d|m$ has the form $d = q^j \delta$ where $0 \le j \le k$ and $\delta | t$. For $d = q^j \delta$, $e(u_1, \frac{m}{d})$ is the order of $u_1 \pmod{\frac{m}{d} = \frac{q^k t}{q^j \delta} = q^{k-j} \frac{t}{\delta}}$. But $u_1 \equiv 1 \pmod{t}$ so the order of $u_1 \pmod{\frac{m}{d}}$ is just the order of $u_1 \pmod{q^{k-j}}$, thus $e(u_1, \frac{m}{d}) = e(u_1, q^{k-j})$. Now $u_1 \equiv g_1 \pmod{q^k}$ shows u_1 is a primitive root mod q^k, hence also a primitive root mod q^{k-j}, so $e(u_1, q^{k-j})$ is just $\phi(q^{k-j})$. Altogether then $e(u_1, \frac{m}{d}) = \phi(q^{k-j})$ and by (4)

$$c(u_1, d) = \frac{\phi(\frac{m}{d})}{\phi(q^{k-j})} = \frac{\phi(q^{k-j} \frac{t}{\delta})}{\phi(q^{k-j})} = \phi\left(\frac{t}{\delta}\right) .$$

For any integer n, $\phi(n)$ is even unless n is 1 or 2. Since t is odd we see that $c(u_1, d) = \phi(\frac{t}{\delta})$ is even unless $\delta = t$. Thus $A(d)$ when $\delta \neq t$, contributes an even number of cycles all of the same length, so contributes $+1$ to sign θ_{u_1}. When $\delta = t$, $d = q^j t$ has $c(u_1, d) = 1$, so $A(d)$ is a single cycle of length $\phi(q^{k-j})$. For $0 \le j \le k-1$, $\phi(q^{k-j})$ is even so we end up with k cycles having even length, which are odd permutations, so sign $\theta_{u_1} = (-1)^k$. (When $j = k$, $d = m$, $A(m)$ is a fixed point, a cycle of length one.) There was nothing special about u_1 so we see that for each i, $1 \le i \le r$, sign $\theta_{u_i} = (-1)^{k_i}$. As soon as one k_i is odd T contains an odd permutation so is even-odd. If all the k_i are even then so are all the θ_{u_i} and the group T they generate is even. But all the k_i are even iff m is a square. But odd m can be a square only when $m \equiv 1 \pmod{4}$. This completes the proof of Theorem 2. □

Proof of Theorem 3.

For $\sigma_g \in \Sigma_R$ we denote the inverse permutation, σ_g^{-1}, by γ_g. Thus $\gamma_g(x) = y$ iff $x = \sigma_g(y)$, or $x \equiv g^y \pmod{p}$. For any subset A of S_{p-1}, A^{-1} denotes the set of inverses of the elements in A. We define $\Gamma_R = \{\gamma_g | g \in R\} = \Sigma_R^{-1}$.

The permutations in these sets satisfy some basic relations which make us introduce further notation. Since $\frac{p-1}{2}$ occurs frequently, we set $q = \frac{p-1}{2}$, $p = 2q + 1$. Paritition X into $I \cup J$ where $I = \{x | 1 \le x \le q\}$ and $J = \{x | q+1 \le x \le p-1\}$. The variables i, j always range over I, J, respectively. Note that $|I| = |J|$, $g^q \equiv -1 \pmod{p}$ for $g \in R$. Define

$$x^* = \begin{cases} x + q, & \text{if } x \in I \\ x - q, & \text{if } x \in J. \end{cases} \tag{5}$$

$x \to x^*$ is a fixed point free involution of X which interchanges I and J. Also $x \to p \to x$ has the same property. We denote these as

$$\eta(x) = x^*, \quad \xi(x) = p - x. \tag{6}$$

Each of η, ξ is a product of q disjoint, hence commuting, transpositions.

$$\begin{aligned} \eta &= \prod_i (i, i^*) = \prod_j (j, j^*), & \eta &= \eta^{-1}, \quad s(\eta) = (-1)^q \\ \xi &= \prod_i (i, p-i) = \prod_j (j, p-j), & \xi &= \xi^{-1}, \quad s(\xi) = (-1)^q. \end{aligned} \tag{7}$$

It may be helpful to get a picture of these, take $p = 11$. We write them out in both cycle and tabular presentation.

$$\eta = (1,6)(2,7)(3,8)(4,9)(5,10) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$
$$\xi = (1,10)(2,9)(3,8)(4,7)(5,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Now $p - \sigma_g(x) \equiv -g^x \equiv g^{x^*} \equiv \sigma_g(x^*) \pmod p$ shows

$$\xi(\sigma_g(x)) = \sigma_g(\eta(x)), \quad \xi\sigma_g = \sigma_g\eta. \tag{8}$$

Taking inverses, or by direct proof, we have

$$\gamma_g(\xi(x)) = \eta(\gamma_g(x)), \quad \gamma_g\xi = \eta\gamma_g. \tag{9}$$

We use these relations to define larger subsets of S_{p-1}:

$$\Sigma = \{\sigma \in S_{p-1} | \xi\sigma = \sigma\eta\}, \quad \Gamma = \{\gamma \in S_{p-1} | \gamma\xi = \eta\gamma\}. \tag{10}$$

Clearly $\Sigma_R \subset \Sigma$, $\Gamma_R \subset \Gamma$ and $\Gamma = \Sigma^{-1}$. We now study the structure of these sets Σ, Γ, as needed for the proof of the theorem. If G is a group and $\zeta \in G$, $C(\zeta)$ denotes the centralizer of ζ in G, the set of elements of G that commute with ζ. With G being S_{p-1} we define

$$A = C(\eta), \quad B = C(\xi). \tag{11}$$

Lemma 1. *Let $\gamma \in \Gamma$, $\alpha \in A$, $\beta \in B$, then $\alpha\gamma \in \Gamma$ and $\gamma\beta \in \Gamma$. If $\sigma \in \Sigma$, then $\sigma\alpha \in \Sigma$ and $\beta\sigma \in \Sigma$.*

Proof. Let $\delta = \alpha\gamma$. Then $\delta\xi = (\alpha\gamma)\xi = \alpha(\gamma\xi) = \alpha(\eta\gamma)$ (by (10)) $= (\alpha\eta)\gamma = (\eta\alpha)\gamma$ (since α commutes with η) $= \eta\delta$, which shows $\delta \in \Gamma$. The proof that $\gamma\beta \in \Gamma$ is similar. The proof for σ is done similarly or follows directly by taking inverses. The results of the lemma can be stated briefly as $A\Gamma B = \Gamma$, $B\Sigma A = \Sigma$. □

We now show how every $\gamma \in \Gamma$ can be brought into a normal form. For any $\tau \in S_{p-1}$, define

$$\begin{aligned} K(\tau) &= \{i | \tau(i) \in J\} = I \cap \tau^{-1}(J) \\ D(\tau) &= \{i | \tau(i) \in I\} = I \cap \tau^{-1}(I). \end{aligned} \tag{12}$$

Thus $K(\tau)$ is the set of those i moved by τ into J while $D(\tau)$ is the set of those i that stay in I under τ. Define

$$r(\tau) = |K(\tau)|. \tag{13}$$

It follows that $|D(\tau)| = q - r(\tau)$. Now $D(\tau^{-1}) = I \cap \tau(I) = \tau(I \cap \tau^{-1}(I)) = \tau(D(\tau))$, which shows $|D(\tau^{-1})| = |D(\tau)|$ from which one has

$$r(\tau^{-1}) = r(\tau). \tag{14}$$

Given $\gamma \in \Gamma$ and $k \in K(\gamma)$, let $m = \gamma(k) \in J$ and let ρ be the transposition (m, m^*). ρ is one of the factors of η, see (7), so $\rho \in A$ and $\gamma' = \rho\gamma \in \Gamma$. Now $\rho\gamma(i) = \gamma(i)$ for $i \neq k$ and $\rho\gamma(k) = m^* \in I$, so γ' moves one less member of I to J, $r(\gamma') = r(\gamma) - 1$. This process may be continued for each element of $K(\gamma)$, so by $r(\gamma)$ successive multiplications of γ on the left by such transpositions, all of which commute with each other so the order in which it is done is immaterial, one obtains a permutation θ having $r(\theta) = 0$. If the product of the transpositions is denoted π, we have

$$\begin{gathered} \theta \in \Gamma, \quad \theta = \pi\gamma, \quad r(\theta) = 0, \\ s(\pi) = (-1)^{r(\gamma)}, \quad s(\theta) = (-1)^{r(\gamma)} \cdot s(\gamma). \end{gathered} \tag{15}$$

θ maps I to I and J to J so let μ be the permutation that is θ restricted to I and is the identity on J. Similarly let ν be θ restricted to J and is the identity on I. Then μ, ν commute and $\theta = \mu\nu = \nu\mu$. Suppose now k, $m \in I$, $k \neq m$. Define $\tau = (k, m)$, $\tau' = (p-k, p-m) = (\xi(k), \xi(m))$. We claim $\tau\tau' \in B$. For $\xi\tau\tau'\xi^{-1} = \xi\tau\xi^{-1} \cdot \xi\tau'\xi^{-1} = (\xi(k), \xi(m))(k, m)$ (since ξ^2 is the identity) $= \tau'\tau = \tau\tau'$ (since τ, τ' are disjoint) which shows $\tau\tau'$ commutes with ξ. By Lemma 1, $\theta\tau\tau' \in \Gamma$. Now write μ^{-1} as a product of transpositions (not necessarily disjoint or commuting) $\tau_1\tau_2 \ldots \tau_n$, say, where $\tau_t = (k_t, m_t)$ for $t = 1, \ldots, n$, and all the elements k_t, $m_t \in I$, since μ^{-1} is the identity on J. Let $\omega_t = \tau_t\tau'_t$ and set $\omega = \omega_1\omega_2 \ldots \omega_n$. Each $s(\omega_t) = 1$, so $s(\omega) = 1$ and each $\omega_t \in B$ so $\omega \in B$. Finally let $\lambda = \theta\omega$, so

$$\lambda \in \Gamma, \quad s(\lambda) = s(\theta) = (-1)^{r(\gamma)} \cdot s(\gamma). \tag{16}$$

$\omega = \tau_1\tau'_1 \ldots \tau_n\tau'_n = \tau_1 \ldots \tau_n\tau'_1 \ldots \tau'_n$ since the τ permutations act only on I while the τ' act only on J. But $\tau_1 \ldots \tau_n = \mu^{-1}$, so $\lambda = \theta\omega = \nu\mu\mu^{-1}\tau'_1 \ldots \tau'_n$, which acts only on J. Thus $\lambda(i) = i$ and λ is a permutation of J. We claim λ is uniquely determined by the fact that $\lambda \in \Gamma$ and λ is the identity on I; thus the intermediate choices of various transpositions, starting from γ, always lead to the same λ. Indeed, since $\lambda \in \Gamma$, $\lambda\xi = \eta\lambda$ so $\lambda\xi(i) = \eta\lambda(i) = \eta(i) = i + q$. Given j, let $i = p - j = \xi(j)$, so $\lambda\xi(i) = \lambda\xi(\xi(j)) = p - j + q$. Since ξ^2 is the identity, $\lambda(j) = p + q - j = 3q + 1 - j$, and λ is uniquely determined. Clearly λ^2 is the identity; λ is an involution on J. λ has a fixed point if $j = 3q + 1 - j$, $j = \frac{3q+1}{2}$, which is an integer iff q is odd. Thus

$$s(\lambda) = (-1)^{\frac{q}{2}} \text{ if } q \text{ is even}, \quad s(\lambda) = (-1)^{\frac{q-1}{2}} \text{ if } q \text{ is odd}. \tag{17}$$

Considering $p \pmod 8$, write $p = 8k + e$, $e = 1, 3, 5, 7$, $q = 4k + \frac{e-1}{2}$, one sees q is even for $e = 1$, $e = 5$ but $\frac{q}{2}$ is even for $e = 1$, odd for $e = 5$. For $e = 3$, $e = 7$, q is odd, but $\frac{q-1}{2}$ is even for $e = 3$, odd for $e = 7$. In summary,

(18) $s(\lambda) = 1$ if $p \equiv 1$ or $3 \pmod 8$, $\quad s(\lambda) = -1$ if $p \equiv 5$ or $7 \pmod 8$.

Noting (16) we now have for any $\gamma \in \Gamma$

$$s(\gamma) = (-1)^{r(\gamma)} \cdot s(\lambda). \tag{19}$$

To complete the proof of Theorem 3 we need:

Lemma 2. *For* $\gamma \in \Gamma$

$$\sum_{i=1}^{q} \gamma(i) = \frac{q(q+1)}{2} + qr(\gamma). \tag{20}$$

Proof. Let $D = D(\gamma)$, $K = K(\gamma)$, $d \in D$, $k \in K$ and $S = \sum_{i=1}^{q} \gamma(i)$; thus $S = \sum_d \gamma(d) + \sum_k \gamma(k)$ and $\gamma(k) \in J$. Then $\gamma(p-k) = \gamma\xi(k) = \eta\gamma(k) = \gamma(k) - q$, so $\gamma(p-k) \in I$, $\gamma(k) = \gamma(p-k) + q$. Thus $S = \sum_d \gamma(d) + \sum_k \gamma(p-k) + qr(\gamma)$. But the numbers $\{\gamma(d), \gamma(p-k)\}$ are q in number, all in I and distinct, since γ is a permutation. Thus $\sum_d \gamma(d) + \sum_k \gamma(p-k) = \sum_{i=1}^{q} i = \frac{q(q+1)}{2}$ so $S = \frac{q(q+1)}{2} + qr(\gamma)$, as claimed. $\square$

Now consider $\left(\frac{p-1}{2}\right)! = q! = \prod_{i=1}^{q} i$. For $g \in R$ and $\gamma_g = \sigma_g^{-1}$ we have $i = \sigma_g(\gamma_g(i)) \equiv g^{\gamma_g(i)} \pmod p$, hence $\prod_{i=1}^{q} i \equiv g^{\sum_i \gamma_g(i)} \equiv g^{\frac{q(q+1)}{2}} (g^q)^{r(\gamma_g)} \pmod p$ by the lemma. Suppose $p \equiv 3 \pmod 4$, q is odd and $\frac{q+1}{2}$ is an integer. Noting $g^q \equiv -1 \pmod p$ gives $q! \equiv (-1)^{\frac{q+1}{2}} (-1)^{r(\gamma_g)} \pmod p$. By (17), since q is odd, $(-1)^{\frac{q-1}{2}} = s(\lambda)$, so $(-1)^{\frac{q+1}{2}} = -s(\lambda)$ so that $q! \equiv -s(\lambda)(-1)^{r(\gamma_g)} \equiv -s(\gamma_g) \pmod p$, by (19). Thus $s(\gamma_g) \equiv -(q!) \pmod p$ and since $s(\sigma_g) = s(\gamma_g)$ we have $s(\sigma_g) \equiv -\left(\frac{p-1}{2}\right)! \pmod p$ which is (2).

Now take $p \equiv 1 \pmod 4$, so q is even. In this case $s(\lambda) = (-1)^{\frac{q}{2}}$, by (17), and so $s(\gamma_g) = (-1)^{r(\gamma_g)}(-1)^{\frac{q}{2}}$, by (19). We've seen $q! \equiv g^{\frac{q(q+1)}{2}} (g^q)^{r(\gamma_g)} \pmod p$. But $g^{\frac{q(q+1)}{2}} = (g^q)^{\frac{q}{2}} g^{\frac{q}{2}} \equiv (-1)^{\frac{q}{2}} g^{\frac{p-1}{4}} \pmod p$, and $(g^q)^{r(\gamma_g)} \equiv (-1)^{r(\gamma_g)}$ thus $q! \equiv g^{\frac{p-1}{4}} (-1)^{\frac{q}{2}} (-1)^{r(\gamma_g)} \equiv g^{\frac{p-1}{4}} s(\gamma_g) \pmod p$. The inverse of $g^{\frac{p-1}{4}} \pmod p$ is $(-1) g^{\frac{p-1}{4}}$ so the above congruence shows $s(\sigma_g) = s(\gamma_g) \equiv -\left(\frac{p-1}{2}\right)! \cdot g^{\frac{p-1}{4}} \pmod p$, completing the proof of Theorem 3. $\square$

We've seen that given $\gamma \in \Gamma$ there are $\alpha \in A$, $\beta \in B$ such that $\alpha\gamma\beta = \lambda$, so $\gamma = \alpha^{-1}\lambda\beta^{-1} \in A\lambda B$, and hence $\Gamma \subset A\lambda B$. On the other hand since $\lambda \in \Gamma$, Lemma 1 shows $A\lambda B \subset \Gamma$. Thus $\Gamma = A\lambda B$, is an $A-B$ double coset. Taking inverses, $\Sigma = \Gamma^{-1} = B^{-1}\lambda^{-1}A^{-1} = B\lambda A$ is a $B-A$ double coset, since A, B are groups and $\lambda = \lambda^{-1}$ Since $\gamma \in \Gamma$ if and only if $\gamma^{-1} \in \Sigma$, we see that any γ in Γ of order two is in $\Gamma \cap \Sigma$; in particular $\lambda \in \Gamma \cap \Sigma$. In general, if a permutation $\pi \in \Gamma \cap \Sigma$ then by the basic relations (10), $\pi\xi = \eta\pi$, so $\pi\xi\pi^{-1} = \eta$ and $\xi\pi = \pi\eta$, so $\pi^{-1}\xi\pi = \eta = \pi\xi\pi^{-1}$. Thus $\pi^2\xi = \xi\pi^2$, hence $\pi^2 \in B$. Similarly $\pi^2 \in A$. Thus $\pi \in \Gamma \cap \Sigma$ implies $\pi^2 \in A \cap B$. The converse is false, take ε to be the identity permutation. Then $\varepsilon^2 \in A \cap B$ but $\varepsilon \notin \Gamma \cap \Sigma$, otherwise that would imply $\xi = \eta$, which is false.

3. The average value of r

Recall that $q = \frac{p-1}{2}$, $I = \{i \mid 1 \le i \le q\}$ and $J = \{j \mid q+1 \le j \le p-1\}$. For each $g \in R$ we have the permutation σ_g and the quantity $r(\sigma_g)$, which is the number of i for which $\sigma_g(i) \in J$. To lighten the notation we now write $r(g)$ for $r(\sigma_g)$. One can also define $r_e(g)$, the number of even i for which $\sigma_g(i) \in J$ and similarly $r_o(g)$, the number of odd i for which $\sigma_g(i) \in J$. Our interest here is in the averages of these quantities taken over all $g \in R$. Thus $\bar{r} = \frac{1}{|R|}\sum\limits_{g\in R} r(g)$ is the average of the numbers $r(g)$. In the same way we have $\bar{r}_e$, $\bar{r}_o$.

Theorem 4. *Let p be a prime ≥ 5; then*

$$\bar{r} = \frac{p+1}{4}. \tag{21}$$

For $p \equiv 1 \pmod 4$

$$\bar{r}_e = \frac{p+3}{8}, \quad \bar{r}_o = \frac{p-1}{8}. \tag{22}$$

Remark 3. We have no information about $\bar{r}_e$, $\bar{r}_o$ when $p \equiv 3 \pmod 4$.

Proof. We make use of the fact that R has a symmetry that allows us to evaluate $\sum\limits_{g\in R} r(g)$. For every $g \in R$, $g^{-1} \equiv g^{p-2} \pmod p$ is also a primitive root since $(p-2, p-1) = 1$. Actually we should write, instead of g^{-1} or g^{p-2}, the value reduced mod p to obtain its representative in X. But this slight carelessness should not lead to any confusion. $g \to g^{-1}$ is an involution on R, with no fixed points, since $g^{-1} \equiv g \pmod p$ implies $g^2 \equiv 1 \pmod p$ which is possible only if $2 \equiv 0 \pmod{p-1}$ which forces $p = 3$, but we have excluded $p = 3$. Note that $\sigma_{g^{-1}}$ should not be confused with $\sigma_g^{-1} = \gamma_g \in \Gamma_R$. Now we claim the following relation holds between $r(g)$ and $r(g^{-1})$:

$$r(g) + r(g^{-1}) = q + 1. \tag{23}$$

Assuming this to be true we can write the sum

$$\sum_{g\in R} r(g) = \sum_{\{g,g^{-1}\}\subset R} (r(g)+r(g^{-1}))$$

where $\{g, g^{-1}\}$ ranges over the $\frac{|R|}{2}$ 2-element subsets $\{g, g^{-1}\} \subset R$. Thus

$$\sum_{g\in R} r(g) = \sum_{\{g,g^{-1}\}\subset R} (q+1) = \frac{1}{2}|R|(q+1)$$

so $\bar{r} = \frac{\frac{1}{2}|R|(q+1)}{|R|} = \frac{q+1}{2} = \frac{p+1}{4}$, proving (21). To prove (23) recall that we introduced for $\tau \in S_{p-1}$, $I = K(\tau) \cup D(\tau)$. Now we introduce $J = K'(\tau) \cup D'(\tau)$ where $K'(\tau) = J \cap \tau^{-1}(I) =$ those j for which $\tau(j) \in I$ and $D'(\tau) = J \cap \tau^{-1}(J) =$ those j for which $\tau(j) \in J$. We claim $|K'(\tau)| = r(\tau)$; for

$$\tau^{-1}(I) = \{x|\tau(x) \in I\} = K' \cup D.$$

Thus $q = |\tau^{-1}(I)| = |K'| \cup |D| = |K'| + q - r(\tau)$, showing $|K'| = r(\tau)$. For any x, $\sigma_{g-1}(x) \equiv g^{-x} \equiv g^{p-1-x} \pmod p$. For $1 \le x \le p-2$ we have $1 \le p-1-x \le p-2$ and for $x = p-1$, $p-1-x = 0 \equiv p-1 \pmod{p-1}$. We define the permutation $\psi \in S_{p-1}$ by $\psi(x) = p-1-x$ for $1 \le x \le p-2$ and $\psi(p-1) = p-1$.

$$\psi = \begin{pmatrix} 1 & 2 & \cdots & q-1 & q & q+1 & \cdots & p-2 & p-1 \\ p-2 & p-3 & \cdots & q+1 & q & q-1 & \cdots & 1 & p-1 \end{pmatrix}$$

and so $\sigma_g\psi(x) \equiv g^{p-1-x} \equiv \sigma_{g^{-1}}(x) \pmod p$. Thus $\sigma_{g^{-1}}(x) = \sigma_g\psi(x) = \sigma_g(p-1-x)$, for $x \ne p-1$ and $\sigma_{g^{-1}}(p-1) = \sigma_g(p-1) = 1$. Now $r(g^{-1})$ is the number of i for which $\sigma_{g^{-1}}(i) \in J$ which is $|K(\sigma_{g^{-1}})|$, or is the number of i for which $\sigma_g\psi(i) \in J$. For $i = q$, $\sigma_g\psi(q) = \sigma_g(q) \equiv g^q \equiv p-1 \pmod p$, so $\sigma_g\psi(q) \in J$. Thus $r(g^{-1}) = 1 +$ the number of $i = 1, 2, \ldots, q-1$ for which $\sigma_{g^{-1}}(i) \in J$. Now for $i = 1, 2, \ldots, q-1$, $j = \psi(i)$ ranges over $p-2$, $p-3$, $\ldots$, $q+1$, which are all of J except for $p-1$ and $\sigma_{g^{-1}}(i) = \sigma_g\psi(i) = \sigma_g(j)$. Thus $\sigma_{g^{-1}}(i) \in J$ iff $\sigma_g(j) \in J$ which means $j \in D'(\sigma_g)$. But $D'(\sigma_g)$ does not contain $p-1$, since $\sigma_g(p-1) = 1$ Thus $K(\sigma_{g^{-1}}) = D'(\sigma_g) \cup \{q\}$ so $r(g^{-1}) = |D'(\sigma_g)|+1 = (q-r(g))+1 = q+1-r(g)$, or $r(g)+r(g^{-1}) = q+1$ as claimed and the proof of (21) is complete.

To prove (22) we make use of another symmetry of R that occurs only when $p \equiv 1 \pmod 4$. In this case $-g \equiv p-g \pmod p$ is also a primitive root because $-g \equiv g^{\frac{p-1}{2}} \cdot g \equiv g^{\frac{p+1}{2}} \pmod p$ and $(\frac{p+1}{2}, p-1) = 1$ since $p \equiv 1 \pmod 4$ means $\frac{p+1}{2}$ is odd. (When $p \equiv 3 \pmod 4$, $\frac{p+1}{2}$ is even and $(\frac{p+1}{2}, p-1) = 2$ so $-g \equiv g^{\frac{p+1}{2}} \pmod p$ is not a primitive root.) Now for i even, $\sigma_{-g}(i) \equiv (-g)^i \equiv g^i \equiv \sigma_g(i) \pmod p$ and so σ_{-g} and σ_g agree on all even i. Thus $r_e(-g) = r_e(g)$. For i odd, $\sigma_{-g}(i) \equiv (-g)^i \equiv -g^i \equiv p - \sigma_g(i) \pmod p$ and since $\sigma_{-g}(i)$, $p-\sigma_g(i)$ both are in X this forces $\sigma_{-g}(i) = p-\sigma_g(i)$ for i odd. Now if i is one of the odd i for which $\sigma_g(i) \in J$, then $\sigma_{-g}(i) =$

$p - \sigma_g(i) \in I$, while if i is one of the odd i for which $\sigma_g(i) \in I$, then $\sigma_{-g}(i) = p - \sigma_g(i) \in J$. Thus of the $\frac{q}{2}$ odd i (since $p \equiv 1 \pmod 4$, $q = \frac{p-1}{2}$ is even) in I, those for which $\sigma_g(i) \in J$ and those for which $\sigma_{-g}(i) \in J$ are disjoint sets and any i belongs to one of these 2 sets. Thus $r_o(g) + r_o(-g) = \frac{q}{2}$. Now we can calculate averages. $\bar{r}_o = \frac{1}{|R|} \sum_{\{g,-g\}} (r_o(g) + r_o(-g))$, where the sum is over the $\frac{1}{2}|R|$ 2-element sets $\{g, -g\} \subset R$, gives $\bar{r}_o = \frac{1}{|R|} \cdot \frac{1}{2}|R| \cdot \frac{q}{2} = \frac{q}{4} = \frac{p-1}{8}$. Finally, since $r(g) = r_e(g) + r_o(g)$, $\bar{r} = \bar{r}_e + \bar{r}_o$ or $\bar{r}_e = \bar{r} - \bar{r}_o = \frac{p+1}{4} - \frac{p-1}{8} = \frac{p+3}{8}$ and the proof of Theorem 4 is finished. $\square$

References

[1] Borevich, A. I.; Shafarevich, I. R. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, 20. *Academic Press, New York-London*, 1966. x+435 pp. MR0195803 (33 #4001), Zbl 0145.04902.

[2] Guy, Richard K. Unsolved problems in number theory. Third edition. Problem Books in Mathematics. Springer-Verlag, New York, 2004. xviii+437 pp. ISBN: 0-387-20860-7. MR2076335 (2005h:11003), Zbl 1058.11001.

[3] Mordell, L. J. *The congruence* $\frac{p-1}{2}! \equiv \pm 1 \pmod p$, *Amer. Math. Monthly* **68** (1961) 145–146. MR0123512 (23 #A837), Zbl 0102.27905.

[4] Tomita, T. Table of class numbers of quadratic fields. http://t-tomita.ceruf/table.html. Last update 3/1/2006. Removed during May 2009.

Joseph Lewittes, Department of Mathematics and Computer Science, Lehman College - CUNY, 250 Bedford Park Boulevard West, Bronx, NY 10468
joseph.lewittes@lehman.cuny.edu

Victor Kolyvagin, The Graduate Center - CUNY, 365 Fifth Avenue, New York, NY 10016
vkolyvagin@gc.cuny.edu

This paper is available via http://nyjm.albany.edu/j/2010/16-16.html.