

**Lemma.** Let  $p$  be an odd prime and  $(a, p) = 1$ . Consider the least positive residues of the integers  $a, 2a, \dots, ((p-1)/2)a$ . Let  $u_1, \dots, u_s$  be those residues which are larger than  $p/2$  and let  $v_1, \dots, v_t$  be the ones smaller than  $p/2$ . For  $i = 1, \dots, s$ , let  $u'_i = u_i - p$ , so that  $-p/2 < u'_i < 0$ . Then the set  $\{-u'_1, \dots, -u'_s, v_1, \dots, v_t\}$  is precisely the set of integers from 1 to  $(p-1)/2$ .

PROOF: There are  $(p-1)/2$  of the integers in question and they are all between 1 and  $(p-1)/2$ . Thus we need only show that they are distinct. Since they are between 1 and  $p$ , it suffices to prove that no two are congruence modulo  $p$ . Now each  $v_i$  is congruent to some  $ja$  modulo  $p$  and each  $-u_i$  is congruent to  $-ka$ , where  $1 \leq j, k \leq (p-1)/2$ . Thus we need to show that  $ja \not\equiv \pm ka$  if  $j \neq k$ . In fact, if  $ja \equiv \pm ka \pmod{p}$  then  $p \mid a(j \pm k)$  and so  $p \mid j \pm k$  since  $(p, a) = 1$ , and thus  $j = k$  since  $|j \pm k| \leq 2(p-1)/2 < p$ .  $\square$

**Lemma.** If  $p$  is an odd prime and  $(a, 2p) = 1$  then  $\left(\frac{a}{p}\right) = (-1)^T$ , where  $T = \sum_{j=1}^{(p-1)/2} [ja/p]$ .

PROOF: Let  $p = 2k + 1$ . Consider the least positive residues modulo  $p$  of the integers  $a, 2a, \dots, ka$ . In other words, these are the values  $ja - p[ja/p]$  for  $j = 1, \dots, k$ . Let  $u_1, \dots, u_s$  be the ones greater than  $p/2$  and  $v_1, \dots, v_t$  be the ones less than  $p/2$ . By Gauss's Lemma (Lemma 9.2),  $\left(\frac{a}{p}\right) = (-1)^s$ . We will now show that  $T \equiv s \pmod{2}$  so that  $(-1)^T = (-1)^s$ .

For  $i = 1, \dots, s$ , let  $u'_i = u_i - p$ , so that  $-p/2 < u'_i < 0$ . By the preceding Lemma,  $\sum_1^s -u'_i + \sum_1^t v_i = \sum_1^k j$ . Thus

$$\begin{aligned} \sum_1^k ja - pT &= \sum_1^k (ja - p[ja/p]) \\ &= \sum_1^s u_i + \sum_1^t v_i \\ &\equiv \sum_1^s -u_i + \sum_1^t v_i \pmod{2} \\ &= -ps + \sum_1^s -u'_i + \sum_1^t v_i \\ &\equiv s + \sum_1^k j \pmod{2} \end{aligned}$$

(using the fact that  $-p \equiv 1 \pmod{2}$ ). This yields  $s \equiv (a-1) \sum_1^k j - pT \equiv T \pmod{2}$ , using the fact that  $a-1 \equiv 0 \pmod{2}$  since  $a$  is odd.  $\square$