

**Homework problem V, due November 16, 11:00 AM**  
Elementary Number theory 2009

Let  $p$  be an odd prime and let  $g$  be a primitive root modulo  $p$ .

- 1) Let  $m$  be a divisor of  $p - 1$ . Show that the order of  $g^m \pmod{p}$  is precisely  $(p - 1)/m$ .
- 2) Let  $m$  be any integer. Show that the order of  $g^m \pmod{p}$  is precisely  $(p - 1)/\gcd(m, p - 1)$ .
- 3) For which  $m$  is  $g^m \pmod{p}$  a primitive root? How many primitive roots modulo  $p$  are there?

Let  $p$  be a prime such that  $p \equiv 1 \pmod{3}$ . In the next two problems you will show, without using quadratic reciprocity, that  $-3$  is a square modulo  $p$ .

- 4) Show that there exists  $a \in (\mathbb{Z}/p\mathbb{Z})^*$  such that  $a$  has order 3.
- 5) Show that  $(a - a^2)^2 \equiv -3 \pmod{p}$  (hence  $-3$  is a square modulo  $p$ ).

In the following two problems you will show that there are infinitely many primes  $p$  with  $p \equiv 1 \pmod{3}$ .

- 6) Let  $x$  be an even integer not divisible by 3. Show that every prime divisor  $p$  of  $x^2 + 3$  satisfies  $p \equiv 1 \pmod{3}$ .
- 7) Show that there are infinitely many primes with  $p \equiv 1 \pmod{3}$ .