

## Number Theory: Examples Sheet 2 of 4

1. Evaluate the following Jacobi symbols (in fact, they are Legendre symbols):

$$\left(\frac{20964}{1987}\right), \quad \left(\frac{741}{9283}\right), \quad \left(\frac{5}{160465489}\right), \quad \left(\frac{3083}{3911}\right).$$

Did it help to know that they are Legendre symbols?

2. Find all odd primes  $p$  for which 21 is a quadratic residue modulo  $p$ .

3. A Mersenne prime is a prime of the form  $2^n - 1$  for some integer  $n \geq 2$ . Prove that 3 is a quadratic non-residue modulo any Mersenne prime strictly greater than 3.

4. Let  $p$  be a prime with  $p \equiv 1 \pmod{4}$ . Prove that the sum of the quadratic residues in the interval  $[1, p-1]$  is equal to the sum of the quadratic non-residues in this interval. Does this hold if  $p \equiv 3 \pmod{4}$ ?

5. Let  $p$  be an odd prime and  $\zeta = e^{2\pi i/p}$ . Let

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

Show that  $\tau^2 = \pm p$ , and determine how the sign depends on  $p$ .

6. Let  $a$  be a positive integer that is not a square. Prove that there are infinitely many odd primes  $p$  such that  $\left(\frac{a}{p}\right) = -1$ .

7. Let  $p$  be a prime with  $p \equiv 3 \pmod{8}$ . Show that

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (2a-p) \left(\frac{a}{p}\right)$$

and

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (p-4a) \left(\frac{a}{p}\right).$$

Deduce that if  $p > 3$  then

$$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) \equiv 0 \pmod{3}.$$

8. Prove that equivalence of binary quadratic forms is an equivalence relation.

9. Are the forms  $3x^2 + 2xy + 23y^2$  and  $2x^2 + 4xy + 5y^2$  equivalent (under the action of  $\mathrm{SL}_2(\mathbb{Z})$ )? Are the forms  $15x^2 - 15xy + 4y^2$  and  $3x^2 + 9xy + 8y^2$  equivalent?

10. Make a list of all reduced positive definite binary quadratic forms of discriminant  $-d$ , where  $d = 8, 11, 12, 16, 19, 23, 163$ .

11. Find the smallest positive integer that can be represented by the form  $4x^2 + 17xy + 20y^2$ . What is the next largest? And the next?
12. Find congruence conditions for a prime  $p$  to be represented by the form  $x^2 + 3y^2$ .
13. Is there a positive definite binary quadratic form that represents 2 and the primes congruent to 1 or 3 modulo 8, but no other primes? Is there such a form representing the primes congruent to 1 modulo 4 only?
14. Find congruence conditions for a positive integer  $n$  to be properly represented by at least one of the two forms  $x^2 + xy + 4y^2$  and  $2x^2 + xy + 2y^2$ .

Assume that  $n$  is coprime to 15, and properly represented by at least one of the forms. Show that congruence conditions modulo 15 allow one to decide which form represents  $n$ .

15. (Optional, for enthusiasts of group theory) Let  $G$  be a group, and  $H$  a subgroup of finite index  $(G : H) = m$ . Write  $G$  as the union of cosets  $x_iH$  ( $1 \leq i \leq m$ ). Then if  $g \in G$ ,  $gx_iH = x_jH$  for some  $j$  (depending on  $g$ ). Write  $\bar{g}$  for the mapping  $i \mapsto j$ . Recall from the proof of Cayley's Theorem that  $\bar{g}$  is a permutation of  $\{1, \dots, m\}$  and that the map  $g \mapsto \bar{g}$  is a homomorphism from  $G$  to the symmetric group  $S_m$ .

From now on, assume that  $H$  is abelian.

- (i) Show that for every  $g \in G$ , the product

$$T(g) = \prod_{i=1}^m x_{\bar{g}(i)}^{-1} g x_i$$

belongs to  $H$ , and that  $T$  is a homomorphism from  $G$  to  $H$  (called the *transfer* homomorphism).

- (ii) Show that if  $G$  is abelian, then  $T(g) = g^m$ .
- (iii) Explain why, when  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  and  $H = \{\pm 1\}$ , (ii) is just Gauss's Lemma.