

## IIA NUMBER THEORY PROBLEM SHEET 1

PROF J.H. COATES

1. Calculate  $d = (a, b)$ , and find integers  $x, y$  such that  $d = ax + by$  in the following cases:-

$$(i) a = 841, b = 160; \quad (ii) a = 2613, b = 2171; \quad (iii) a = 8991, b = 3293.$$

2. Let  $a, b$  be positive integers with  $a > b > 1$ . Let  $\lambda(a, b)$  be the number of steps (i.e. individual applications of the Euclidean algorithm) required to compute  $d = (a, b)$  via successive applications of the Euclidean algorithm. Clearly  $\lambda(a, b) < b$ . Prove the stronger estimate

$$\lambda(a, b) \leq 2 \left\lceil \frac{\log b}{\log 2} \right\rceil$$

3. (i) Suppose that  $n$  is known to be the product of two primes. Show how one can determine these primes from the knowledge of  $n$  and  $\varphi(n)$ .

(ii) Suppose that  $n$  is not a perfect square, and satisfies  $n - n^{2/3} < \varphi(n) < n - 1$ . Deduce that  $n$  is the product of two distinct primes.

4. Let  $p$  be a prime dividing  $b^n - 1$ , where  $b, n$  are integers  $> 1$ . Show that either  $p \equiv 1 \pmod n$ , or  $p$  divides  $b^d - 1$  for some proper divisor  $d$  of  $n$ . Using this remark, find the prime factorizations of

$$2^{11} - 1 = 2047, \quad 3^{12} - 1 = 531440, \quad 2^{35} - 1 = 34359738367$$

5. (i) Find the smallest non-negative integer  $x$  satisfying

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod 11, \quad x \equiv 5 \pmod 16$$

(ii) Find the smallest non-negative integer  $x$  satisfying

$$19x \equiv 103 \pmod 900, \quad 10x \equiv 511 \pmod 841$$

6. Let  $A$  be the group  $(\mathbb{Z}/65520\mathbb{Z})^\times$ . Determine the least positive integer  $n$  such that  $g^n = 1$  for all  $g \in A$ .

7. Six lecturers begin their courses of lectures on Monday, Tuesday, Wednesday, Thursday, Friday and Saturday, and announce their intentions of lecturing at intervals of two, three, four, one, six and five days, respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six lectures be compelled to omit a lecture?

8. Prove that  $-2$  is a primitive root modulo 23. Determine all solutions of the congruence  $x^7 \equiv 17 \pmod{23}$ , and of the congruence  $x^{26} \equiv 10 \pmod{23}$ .

9. Find a generator of  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  for  $p = 5, 7, 11, 13$ , and for all integers  $n \geq 1$ .

10. Let  $n$  be an odd positive integer. Prove there is a 1-1 correspondence between the factorization of  $n$  of the form  $n = ab$ , where  $a \geq b \geq 1$ , and representations of the form  $t^2 - s^2$ , where  $s$  and  $t$  are integers  $\geq 0$ . Use this remark to factor 9271 and 200819.

11. Evaluate the following Legendre symbols:-

$$\left(\frac{20964}{1987}\right), \quad \left(\frac{4977}{1987}\right), \quad \left(\frac{7411}{9283}\right), \quad \left(\frac{5}{160465489}\right), \quad \left(\frac{3083}{3911}\right).$$

(You may use reciprocity for the Jacobi symbol to shorten the calculation)

12. Let  $p = 2081$  (a prime). Find a square root of 302 modulo  $p$  (see Koblitz, p. 47 & 48).