NUMBERS AND SETS EXAMPLES SHEET 3. W. T. G.

1. Solve (ie., find all solutions of) the equations

(i) $7x \equiv 77 \pmod{40}$.

(ii) $12y \equiv 30 \pmod{54}$.

(iii) $3z \equiv 2 \pmod{17}$ and $4z \equiv 3 \pmod{19}$.

2. Without using a calculator, work out the value of $17^{10,000} \pmod{31}$.

3. Again without using a calculator, explain why 23 cannot divide $10^{881} - 1$.

4. Let $a_1 = 6$ and for $n > 1$ let $a_n = 6^{a_{n-1}}$. What is $a_{2002} \pmod{91}$?

5. An RSA encryption scheme (n, d) has modulus $n = 187$ and coding exponent $d = 7$. Factorize n, and hence find a suitable decoding exponent e. If you have a calculator, check your answer by encoding the number 35 and then decoding the result.

6. Let p be a prime number and let $1 \leqslant k < p$. Prove that $\binom{p}{k}$ is a multiple of p. If you use any results from the course, make clear what they are and how you are using them.

7. Let P be a polynomial of the form

$$P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 \ ,$$

where the coefficients a_i are all integers. Suppose that r and s are coprime positive integers and that $P(r/s) = 0$. Prove that $s = 1$, again making clear what results you use in the process. Deduce that every root of P is either an integer or an irrational number.

8. Let p be a prime and let $\mathbb{Z}_p^*$ stand for the set of non-zero integers mod p. Let $a \in \mathbb{Z}_p^*$. Prove that the function f defined by $f(x) = ax$ is a bijection from $\mathbb{Z}_p^*$ to itself. By considering the product $f(1)f(2)\ldots f(p-1)$ give another proof of Fermat's little theorem. Adapt your argument to prove Euler's theorem as well.

9. Let a and b be positive integers with $(a, b) = 1$. Prove that $\phi(ab) = \phi(a)\phi(b)$. (This should be done from first principles - i.e., without using the fundamental theorem of

arithmetic or the calculation of ϕ given in lectures.) Show that this gives another way to establish the value of $\phi(m)$, given the prime factorization of m.

10. Let p be an odd prime. An element $x \neq 0$ of $\mathbb{Z}_p$ is a *quadratic residue* if it is a square - that is, if there exists $y \in \mathbb{Z}_p$ such that $y^2 = x$. Prove that exactly $(p-1)/2$ elements of $\mathbb{Z}_p$ are quadratic residues.

11. Let p be an odd prime. Deduce from Wilson's theorem that -1 is a quadratic residue mod p if p is of the form $4n+1$. Prove that -1 is not a quadratic residue mod p if p is of the form $4n+3$.

12. Prove that x is a quadratic residue mod p if and only if $x^{(p-1)/2} \equiv 1 \pmod{p}$. (This gives a second proof of the result of 10.)

13. Let p be a prime of the form $3k+2$. Show that the only solution to $x^3 = 1$ in $\mathbb{Z}_p$ is $x = 1$. Deduce, or prove directly, that every element of $\mathbb{Z}_p$ has a cube root.

14. By considering numbers of the form $(2p_1p_2 \ldots p_k)^2 + 1$, prove that there are infinitely many primes of the form $4n+1$.

15. Show that 19^{19} is not the sum of a fourth power and a (positive or negative) cube.

16. Let $n \geq 2$ be a positive integer such that we have $a^{n-1} \equiv 1$ (n) for every a coprime to n. Must n be prime?

17. (Not hard, but optional.) Prove that addition of positive integers is associative, and prove the cancellation law for addition ($a + c = b + c$ implies that $a = b$), starting from the Peano axioms.