

Number Theory: Problem sheet 2

Solutions must be submitted by Thursday 10 March 2005

1. Prove that if a is odd then $a^2 \equiv 1 \pmod{8}$.
Also prove that if b is coprime to 6 then $b^2 \equiv 1 \pmod{24}$. [6]
2. Let n be even. Prove that if $a \equiv b \pmod{n}$ then $a^2 \equiv b^2 \pmod{2n}$. [4]
3. Solve the following linear congruences (that is, find the general solution, or prove that no solution exists):
 - (i) $7x \equiv 3 \pmod{17}$;
 - (ii) $12x \equiv 16 \pmod{45}$;
 - (iii) $69x \equiv 21 \pmod{111}$;
 - (iv) $79x \equiv 201 \pmod{271}$;
 - (v) $627x \equiv 308 \pmod{1001}$. [10]
4. Prove that there are infinitely many prime numbers p satisfying $p \equiv 5 \pmod{6}$. [6]
5. Show that if n is a composite number, then $(n-1)! \equiv 0 \pmod{n}$ except for one value of n , which you should determine.
Thus one can test whether a number is prime by computing $(n-1)!$ modulo n . Is this a useful way of testing primality? [6]
6. Let n and k be integers with $n \geq 2$ and $k \geq 2$. Prove that $(n-1) \mid (n^k - 1)$. Deduce that if $n^k - 1$ is prime then $n = 2$ and k is prime.
The MAPLE command `isprime` tests a number for primality and the command `ifactor` splits it into its prime factors. For each prime p with $p \leq 30$ determine whether $2^p - 1$ is prime, and if not find its least prime factor. (You are advised to use MAPLE for the higher values of p .)
Primes of the form $2^p - 1$ are called Mersenne primes. The largest known prime is the Mersenne prime $2^{24036583} - 1$. Determine, explaining your method, how many decimal digits it has. (A 10-digit pocket calculator should suffice for this!) [19]
7. In each case find the least nonnegative residue of a modulo p . (Note that each p is prime.)
 - (i) $a = 3^{2005}$, $p = 7$; (ii) $a = 7^{2048}$, $p = 13$; (iii) $a = 3^{1000}$, $p = 17$. [9]

8. Solve, whenever possible, each of the following systems of simultaneous congruences:
- (i) $x \equiv 10 \pmod{11}$, $x \equiv 16 \pmod{19}$;
 - (ii) $x \equiv 4 \pmod{21}$, $x \equiv 22 \pmod{39}$;
 - (iii) $x \equiv 97 \pmod{105}$, $x \equiv 100 \pmod{161}$;
 - (iv) $16x \equiv 27 \pmod{37}$, $23x \equiv 16 \pmod{47}$;
 - (v) $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{11}$, $x \equiv 2 \pmod{13}$. [12]
9. Use the Chinese Remainder Theorem to find all solutions of the following congruences:
- (i) $x^2 \equiv 1 \pmod{95}$;
 - (ii) $x^2 \equiv -1 \pmod{145}$;
 - (iii) $x^2 \equiv 1 \pmod{165}$. [12]
10. Recall that the order of a modulo p is the smallest positive integer k with $a^k \equiv 1 \pmod{p}$. Make a table of the orders of all integers $1 \leq a \leq 18$ modulo 19. Also, find the inverse of each a modulo 19.
- In each case compare the order of a and its inverse modulo 19. What do you notice? Prove that this observation holds in general (that is, with an arbitrary prime p in place of 19.) [16]
11. (Challenge problem) Show that if n is an integer with $n \geq 2$ then $n \nmid (2^n - 1)$.