

Number Theory: Problem sheet 3

Solutions must be submitted by Thursday 28 April 2005

1. Find one primitive root for each of the following primes: (i) 19, (ii) 23, (iii) 61. [9]
2. Find all solutions of the congruence $x^7 \equiv 1 \pmod{2003}$. (Note that 2003 is prime. It may help to use MAPLE for your calculations.) [6]
3. Using a primitive root of 19, or otherwise, find all solutions of the following congruences:
(i) $x^5 \equiv 2 \pmod{19}$;
(ii) $x^4 \equiv 2 \pmod{19}$;
(iii) $x^{10} \equiv 4 \pmod{19}$. [9]
4. Recall that if n has the prime factorization $n = \prod_{j=1}^n p_j^{e_j}$ then $\varphi(n) = \prod_{j=1}^n (p_j - 1)p_j^{e_j-1}$. It follows that for primes p , $p \mid n$ implies that $(p-1) \mid \varphi(n)$ and $p^2 \mid n$ implies that $p \mid \varphi(n)$.
Find all $n \in \mathbf{N}$ for which $\varphi(n) = 4$. Similarly find all $n \in \mathbf{N}$ with $\varphi(n) = 8$ and all $n \in \mathbf{N}$ with $\varphi(n) = 10$. [11]
5. Prove that if $m \mid n$ then $\varphi(m) \mid \varphi(n)$. [Hint: think about the prime factorizations of m and n .] [6]
6. Find all solutions of each of the following congruences:
(i) $x^2 \equiv 5 \pmod{11^3}$,
(ii) $x^2 \equiv -1 \pmod{17^3}$,
(iii) $x^3 \equiv 7 \pmod{3^4}$,
(iv) $x^2 - x - 1 \equiv 0 \pmod{19^2}$,
(v) $x^3 \equiv 1 \pmod{19^3}$. [19]
7. Let $n \in \mathbf{N}$ and let $c_n = (6n+1)(12n+1)(18n+1)$. Prove that if each of $6n+1$, $12n+1$ and $18n+1$ is a prime number then c_n is a Carmichael number, that is $a^{c_n-1} \equiv 1 \pmod{c_n}$ for all a coprime to c_n . [Hint: by the Chinese remainder theorem it suffices to prove that $a^{c_n-1} \equiv 1 \pmod{p}$ for $p = 6n+1$, $p = 12n+1$ and $p = 18n+1$.]
As 7, 13 and 19 are all prime, $c_1 = 1729$ is a Carmichael number. Find the least $n \geq 2$ with all of $6n+1$, $12n+1$ and $18n+1$ prime and calculate the corresponding c_n . [8]

8. A *perfect number* is a natural number n whose positive divisors (excluding n itself) add up to n . Thus, for example, 28 is a perfect number since $1 + 2 + 4 + 7 + 14 = 28$. Using the result of sheet 1, Q.9, prove that $2^{k-1}(2^k - 1)$ is perfect whenever $2^k - 1$ is prime. From sheet 2, Q.6, find all perfect numbers of this form with $k \leq 30$. [10]

[Euler proved that every even perfect number has the form $2^{k-1}(2^k - 1)$ with $2^k - 1$ prime. It is still unknown whether there are any odd perfect numbers.]

9. Let m be an odd number with $m > 1$. Suppose that $a^2 \equiv b^2 \pmod{m}$ and that $a \not\equiv \pm b \pmod{m}$. Prove that $g = \gcd(m, a - b)$ satisfies $1 < g < m$ and so given such a , b and m we may swiftly find a factorization of m .

Use this method (and MAPLE) to find non-trivial factors of m given

- (i) $m = 7313$, $a = 100$, $b = 2372$;
- (ii) $m = 10308049$, $a = 234329$, $b = 448038$;
- (iii) $m = 1000549096994267$, $a = 313131313131313$, $b = 540380072548603$. [13]

10. Apply the Fermat test, by hand, to each of the following numbers n with base a :

- (i) $n = 257$, $a = 3$;
- (ii) $n = 1201$, $a = 2$;
- (iii) $n = 1729$, $a = 2$.

In each case, what do you conclude? [9]

11. (Challenge problem) For $n \in \mathbf{N}$ the n -th Fermat number is $F_n = 2^{2^n} + 1$. Prove that if p is a prime factor of F_n then $p \equiv 1 \pmod{2^{n+1}}$.