The following questions count for assessment: 1, 2, 3, 4, 5, 7, 9. These are marked *. Please hand in your solutions, via the Coursework Box on Level 8 of the Laver Building, by Friday 17th January.

1*. Let the order of a modulo n be k. Show that the order of a^r modulo n is $k/\gcd(r,k)$. **[7]**

2*. For $n = 13$, $n = 16$, and $n = 20$, find the order modulo n of all a with $1 \leq a < n$ and $\gcd(a,n) = 1$. [In each case, first find $\varphi(n)$, which is the number of a. All the orders will divide this. The result in Question 1 should also save you some time.] **[15]**

3*. Using the Theorem on the existence of primitive roots, decide for each of the values $n = 10, 11, 12, 13, 15, 18, 25, 37, 41, 49, 81, 125$ whether a primitive root mod n exists. In each case where primitive roots do exist, find one of the primitive roots, and determine how many of the numbers a with $1 \leq a < n$ are primitive roots. (You do not need to find all of the primitive roots.) **[24]**

4*. Write out a table of the powers of the primitive root 5 modulo 23. Use it to find all solutions of the following congruences:

(i) $x^5 \equiv 13 \pmod{23}$;
(ii) $x^{14} \equiv 5 \pmod{23}$;
(iii) $x^8 \equiv 18 \pmod{23}$;
(iv) $9x^7 \equiv 2 \pmod{23}$.

[16]

5*. Determine how many incongruent solutions there are to each of the following congruences. (You do not have to find the solutions. There is no need to look for primitive roots.)

(i) $x^3 \equiv 11 \pmod{19}$;
(ii) $x^6 \equiv 18 \pmod{19}$;
(iii) $x^{21} \equiv 12 \pmod{29}$;
(iv) $x^{17} \equiv 5 \pmod{43}$.

[12]

6. (a) Let p be prime and let a have order 3 modulo p. Use the identity $a^3 - 1 = (a-1)(a^2+a+1)$ to show that $a^2 + a + 1 \equiv 0 \pmod{p}$. Set $b = 2a+1$. Show that $b^2 \equiv -3 \pmod{p}$ and that $a+1$ has order 6 modulo p.
(b) Conversely, suppose that $p \geq 5$ is prime and that there exists an integer b with $b^2 \equiv -3 \pmod{p}$. Write $h = (p+1)/2$ so $2h \equiv 1 \pmod{p}$, and set $a = (b-1)h$. Show that a has order 3 modulo p, and deduce that $p \equiv 1 \pmod{3}$.

7*. Show by induction that $5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}$ for $n \geq 3$. Deduce that 5 has order 2^{n-2} modulo 2^n. **[10]**

8. Let $p \equiv 2 \pmod{3}$ be prime. Show that the congruence $x^3 \equiv a \pmod{p}$ has solution $x \equiv a^{(2p-1)/3} \pmod{p}$. Is this solution unique mod p? Can you find a similar formula for the solution of $x^5 \equiv a \pmod{p}$ when p is a prime with $p \equiv 2 \pmod{5}$?

9*. (a) Let p be an odd prime and set $M_p = 2^p - 1$ (the pth Mersenne number). Show that if q is a prime factor of M_p then 2 has order p modulo q, and deduce that $q \equiv 1 \pmod{2p}$. (For example, $M_{11} = 23 \times 89$ has both prime factors $\equiv 1 \pmod{22}$).
(b) Use the result of part (a) to show that M_{13} and M_{17} are both prime, and to find a prime factor of each of M_{23} and M_{29}. [You do not have to compute M_p in each case; it is enough to show that $2^p \equiv 1 \pmod{q}$. If M_p is composite, it will have a prime factor $q < \sqrt{M_p}$, so you only need to consider q up to that bound.] **[16]**

Nigel Byott
December 2002