First Arts Modular Degree

Mathematical Studies 2004–2005

Combinatorics and Number Theory Solution Sheet 4

1. As

$$n\binom{n-1}{m-1} = m\binom{n}{m},$$

n divides $m\binom{n}{m}$. Now we are assuming that m and n are relatively prime and so it follows that n must divide $\binom{n}{m}$. Note that what we have proved may not be true if $\gcd(m,n) > 1$.

2. Using the Euclidian algorithm for 31 and 41, we have $1 = 4 \times 31 - 3 \times 41$. This means that

$$31 \times 4 \equiv 1 \bmod 41.$$

Multiplying by 3,

$$31 \times 12 \equiv 3 \bmod 41$$

and we therefore take $x = 12$.

3. Using the Euclidian algorithm for 317 and 409, we have $1 = 40 \times 317 - 31 \times 409$. This means that

$$317 \times 40 \equiv 1 \bmod 409.$$

Multiplying by 3,

$$317 \times 120 \equiv 3 \bmod 409$$

and we therefore take $x = 120$.

4. Suppose that $\gcd(b,c) = 1$ and let $d = \gcd(b^m, c^n)$. Suppose that $d > 1$. Then there is a prime p dividing d which divides both b^m and c^n. However, as p is a prime, if p divides b^m, p divides b. Likewise, if p divides c^n, p divides c. But then p is a common divisor of b and c, contradicting $\gcd(b,c) = 1$. Therefore, $d = 1$.

5. As

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r},$$

all three binomial coefficients cannot be odd, for the sum of two odd numbers is even.

6. There does not seem to be a quick way to do this question. We calculate as follows:

$$2^6 = 64 \equiv 17 \bmod 47, \quad 2^{12} \equiv 17^2 \equiv 289 \equiv 7 \bmod 47$$
$$2^{18} \equiv 17 \times 7 \equiv 119 \equiv 25 \bmod 47, 2^{20} \equiv 100 \equiv 6 \bmod 47$$

We therefore take $x = 6$.

7. The order is a divisor of 30. Note that

$$3^5 = 243 \equiv -5 \bmod 31, \quad 3^{10} \equiv 25 \bmod 32, \quad 3^{15} \equiv -125 \equiv -1 \bmod 31.$$

As the order of 3 modulo 31 is not 2 or 3, these calculations show that 3 must have order 30 modulo 31.

8. We have

$$a^{p-1} \equiv 1 \bmod p$$

or equivalently,

$$a^{p-1} - 1 \equiv 0 \bmod p.$$

Thus p divides $a^{p-1} - 1$. But $a^{p-1} - 1$ factorizes as

$$a^{p-1} - 1 = (a-1)(a^{p-2} + a^{p-3} + \cdots + a + 1$$

and hence p divides this product. But as p is a prime, p must divide one of the two factors above. However, p cannot divide $a - 1$, as we have excluded the possibility $a \equiv 1 \bmod p$. Hence the other possibility holds, meaning that

$$a^{p-2} + a^{p-3} + \cdots + a + 1 \equiv 0 \bmod p.$$

9. We have

$$2^{p-1} \equiv 1 \bmod p$$

and since $p - 1$ is even,

$$2^{2(p-1)/2} = 4^{(p-1)/2} \equiv 1 \bmod p.$$

This implies that the order of 4 modulo p is a divisor of $(p-1)/2$.

10. As n has order 2 modulo p, $n^2 \equiv 1 \bmod p$. This means p divides $n^2 - 1 = (n-1)(n+1)$. As p is a prime, p divides either $n - 1$ or $n + 1$. Now if p divides $n - 1$, $n \equiv 1 \bmod p$ and this means that n has order 1 modulo p. Since n has order 2, we must have the other case, namely, p divides $n + 1$, or equivalently, $n \equiv -1 \bmod p$.