Tutorial 1

Main topics: Greatest common divisors, Euclid's algorithm, arithmetic modulo m.

1. Write down all the common divisors of 56 and 72.

2. Let a, b, and c be integers. If $a \,|\, b$ and $a \,|\, c$, prove that $a^2 \,|\, b^2 + 3c^2$.

3. (a) Use Euclid's algorithm to find $d = \gcd(323, 377)$.
   (b) Find integers x, y such that $323x + 377y = d$.

4. Simplify the following, giving your answers in the form $a \pmod m$ where $0 \leq a < m$.
   (a) $14 \times 13 - 67 + 13^3 \pmod{10}$
   (b) $5^3 \pmod 7$
   (c) $5^3 + 2 \times 4 \pmod 7$
   (d) $21 \times 22 \times 23 \times 24 \times 25 \pmod{20}$

5. (a) Calculate $3^2, 3^4, 3^8, 3^{16}, 3^{32}, 3^{64}, 3^{128}$ and 3^{256} modulo 19.
   (b) Use these to calculate 3^{265} modulo 19. (Hint: $265 = 256 + 8 + 1$.)
   [Write your answers in the form $0, 1, \ldots, 18 \pmod{19}$.]

6. (A test for divisibility by 11.)
   Let $n = a_d a_{d-1} \ldots a_2 a_1 a_0$ be a positive integer written in base 10, i.e.
   $$n = a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^d a_d,$$
   where $a_0, a_1, \ldots a_d$, are the digits of the number n read from right to left.
   (a) Show that $n \equiv a_0 - a_1 + a_2 - a_3 \ldots + (-1)^d a_d \pmod{11}$. Hence n is divisible by 11 exactly when $a_0 - a_1 + a_2 - a_3 \ldots + (-1)^d a_d$ is divisible by 11.
   (b) Use this test to decide if the following numbers are divisible by 11:
   (i) 123537 (ii) 30639423045.

7. Prove that if $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

8. Write down the addition and multiplication tables for $\mathbb{Z}/7\mathbb{Z}$.
   Hence write down the multiplicative inverse of 2 in $\mathbb{Z}/7\mathbb{Z}$.
   (**Note:** Here we use a as an abbreviation for $[a]_m$ to simplify notation.)

9. Find the smallest positive integer in the set $\{6u + 15v \mid u, v \in \mathbb{Z}\}$. Justify your answer.

10. Prove that if a, b, c are integers with $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod m$.
    Give an example to show that this result fails if we drop the condition that $\gcd(c, m) = 1$.
    What can you conclude if $\gcd(c, m) = d$?

11. (a) Show that if p is prime, then p divides the binomial coefficient
    $$\binom{p}{k} = \frac{p!}{k!(p-k)!} \qquad \text{for} \qquad 0 < k < p$$
    (b) Deduce, using induction on n and the binomial theorem, that if p is prime then $n^p \equiv n \pmod p$ for all natural numbers n ("Fermat's Little Theorem").