Tutorial 2

Main topics: Fields, RSA cryptography

1. Which of the following are fields (using the usual definitions of addition and multiplication)?
   (a) The positive real numbers.
   (b) $\{a\sqrt{2} \mid a \in \mathbb{Q}\} \subset \mathbb{R}$
   (c) $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$
   (d) $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$

2. (Fields have no zero divisors)
   (a) Using the field axioms, show that in any field K: $c \times 0 = 0$ for all $c \in K$.
   (b) Using the field axioms, show that in any field: if $ab = 0$ then $a = 0$ or $b = 0$.
   (c) Show that $\mathbb{Z}/9\mathbb{Z}$ is not a field.

3. (Solving equations in fields)
   (a) Find all solutions to the following equations in $\mathbb{F}_7$: (i) $x^2 = [2]_7$ (ii) $x^2 = [3]_7$
   (b) Is $\mathbb{F}_7$ algebraically closed?
   (c) Factor the polynomial $x^2 - [2]_7$ over $\mathbb{F}_7$ (into a product of linear polynomials).

4. (a) Find the (multiplicative) inverse of 24 in $\mathbb{Z}/35\mathbb{Z}$.
   (b) What is the (multiplicative) inverse of 35 in $\mathbb{Z}/24\mathbb{Z}$?
   (c) Solve the following equation in $\mathbb{Z}/35\mathbb{Z}$: $24x + 5 = 0$

5. (Fermat's Little Theorem)
   (a) Simplify the following: $3^{52} \pmod{53}$.
   (b) Calculation shows that $2^{147052} \equiv 76511 \pmod{147053}$.
   What can you conclude about 147053?

6. Use Euler's Theorem to calculate $30^{62} \pmod{77}$

7. (RSA Cryptosystem)
   Let $m = 3 \times 19 = 57$.
   a) Show that $e = 5$ is a suitable choice of encrypting key.
   b) With this encrypting key, encrypt the message '2 3 6 18'.
   c) Calculate the decrypting key d (for $e = 5$).
   d) With this decrypting key, decrypt the message '7 50'.