Review for Exam 2

1. **Prove:** If a, $b \in \mathbb{Z}$ are relatively prime, then for every $c \in \mathbb{Z}$ there exist integers s and t so that $c = sa + tb$.

2. Let p be a prime number. Show that if p divides the product ab, then p divides a or p divides b.

3. Find all associates of 6 in $\mathbb{Z}_{10}$.

4. Find all greatest common divisors of $11 + 2i$ and $-7 + i$ in $\mathbb{Z}[i]$ and give a Bezout-equation for one of them.

5. **Prove:** If $a \neq 0$ is *not* a zero-divisor in a commutative ring R and if there are x and y in R so that $ax = ay$, then it is $x = y$.

6. Let a, b be integers and p be a prime number.
Prove: If $a^2 \equiv b^2 \pmod{p}$, then p divides $a - b$ or p divides $a + b$.

7. Let R be a commutative ring. Assume that for two elements a, $b \in R$ we know that a, b, and $a + b$ are all units in R. Show that then also $a^{-1} + b^{-1}$ is a unit in R.
[Hint: Calculate the fraction $\frac{1}{a} + \frac{1}{b}$.]

8. Consider the ring $\mathbb{Z}_{27}$.

(a) List all units.

(b) Find the inverse of the element 16 in $\mathbb{Z}_{27}$ and give the result as a number between 1 and 26.

(c) Calculate $\frac{13}{16}$.

(d) List the powers of 2 and find the order of the element 2. [Part (a) gives you a hint for what the order of 2 could be.]

(e) What is the order of 25?

9. **(a)** Define carefully the notion of a zero-divisor.

(b) Show that if the integers a and n are *not* relatively prime, then a is a zero-divisor in $\mathbb{Z}_n$.

(c) What do you know about a as an element of $\mathbb{Z}_n$, if a and n are relatively prime?

(d) Conclude from (a) and (b) that a is a zero-divisor in $\mathbb{Z}_n$ exactly when a and n are not relatively prime.

10. Consider the ring $\mathbb{Z}_{37}$. The order of 2 is 36 in this ring (You don't have to check this!).

(a) Find an element a of order 4.

(b) Give both square roots of -1.

11. (a) Show that the polynomial $p(X) = 3X^3 + 2X^2 - 4X + 2$ has no roots in $\mathbb{Z}$.

(b) Show that $\frac{3}{5}$ is not a root of a monic polynomial with integer coefficients.

12. Show that there exists no element $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ with the property $(a + b\sqrt{2})^k = 1 + \sqrt{2}$ for some $k > 1$.

13. Suppose $\mathbb{Z}_p$ contains a unit of order 5. Show that $p = 1 + 10k$ for some $k \in \mathbb{Z}$.
The first such prime is $p = 11$. What is the next such prime? Can you find a unit of order 5 in the ring $\mathbb{Z}_p$ for your p?

14. Let $a = 21$ and $b = 40$.

(a) Find x, $y \in \mathbb{Z}$ so that

$$x \equiv 1 \pmod{21}, \qquad x \equiv 0 \pmod{40}, \qquad y \equiv 0 \pmod{21}, \qquad y \equiv 1 \pmod{40}$$

(b) Find $z \in \mathbb{Z}$ so that simultaneously

$$z = 3 + 21k \quad \text{and} \quad z = 2 + 40l$$

for some choice of k, $l \in \mathbb{Z}$.