5) Find by hand integers $s$ and $t$ such that $1 = 5s + 7t$. Show that $s$ and $t$ are not unique. What is (for a fixed pair $(s, t)$) the gcd of $s$ and $t$?

7) a) Show that the ISBN-10 check digit will discover all accidental exchanges of adjacent numbers. (Hint: If the numbers are $b, c$, the part of the ISBN calculation is $(a + 1)b + ac$, where $a$ depends on the position. Show that it is not possible for $(a + 1)b + ac \equiv (a + 1)c + ab \pmod{11}$.)
b) Does the ISBN-13 also detect exchanges of adjacent numbers? Give a proof, or a counterexample. (Hint: If you use the same approach, as in a), you end up e.g. with an equation $3b + c = 3c + b$. Then use the fact that $2 \cdot 5 \equiv 0 \pmod{10}$.)

8) Calculate the gcd of $x^4 + 4x^3 - 13x^2 - 28x + 60$ and $x^6 + 5x^5 - x^4 - 29x^3 - 12x^2 + 36x$.

9) a) Solve the equation $(7x + 15) \mod{31} = 14$.
b) Find (for example by trying out all values of $x$) all solutions to the equation $x^2 \mod 7 = 2$.
c) Find all solutions to the equation $x^2 \mod 7 = 3$.
d) Find all solutions to the equation $x^2 \mod 8 = 1$.
e) Based on the results in b-d), what can you say about the number of solutions for quadratic equations modulo a prime?

10) Show that it is not possible to define a division with remainder (i.e. write $a = qb + r$ with $r < b$) in the set of polynomials in two variables. (Hint: What would be the remainders when dividing $x$ by $y$, and when dividing $y$ by $x$? What does this imply for the ordering?)
(Note: This means we cannot use the Euclidean algorithm for multivariate polynomials. Nevertheless it makes sense to talk about a gcd of multivariate polynomials, we just can't find it easily.)

11+) Let $p(x) = x^3 - 6x^2 + 12x - 3$ and $\alpha \in \mathbb{R}$ a root of $p(x)$. (Calculus shows there is only one real root.)
a) Let $f(x) \in \mathbb{Q}[x]$ be any rational polynomial and $g(x) = f(x) \mod p(x)$. Show that $f(\alpha) = g(\alpha)$.
(Note: We can therefore calculate with polynomials modulo $p(x)$ and have $x$ play the role of $\alpha$ — for example when calculating $\alpha^5$ we note that $x^5 \mod p(x) = 75x^5 - 270x + 72$, therefore $\alpha^5 = 75\alpha^5 - 270\alpha + 72$.)
b) Calculate $(x - 2)^3 \mod p$. What can you conclude from this about $\alpha$?

12+) Show that there must be a power of 3 (with exponent $\geq 1$, i.e. we exclude $3^0$) whose last four digits are 0001. Hint: consider the sequence

$$3 \mod 10000, 3^2 \mod 10000, 3^3 \mod 10000, 3^4 \mod 10000, 3^5 \mod 10000, \ldots$$

Show that this sequence must be eventually periodic, i.e. there are $m < n$ such that $3^m \equiv 3^n \pmod{10000}$. Then, using the invertability of 3 modulo 10000, show that one can go “backwards” from $3^k$ to $3^{k-1}$. Conclude that therefore there must be an $l$, such that $3^l \equiv 3 \pmod{10000}$ and that $3^{l-1}$ has last digits 0001.

14) (GAP) In this problem we are working modulo 3. Consider the polynomial $f(x) = x^2 - 2$.
a) Determine the nine possible remainders when dividing any polynomial by $f$ modulo 3.
b) Let $R$ be the set of these remainders with addition and multiplication modulo $f$ and modulo 3. Construct the addition and multiplication table.
15) Consider the set \( R = \{ (a, b) \mid a, b \in \mathbb{Z} \} \). We define an addition and a multiplication by

\[
(a, b) + (c, d) = (a + c, b + d) \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc)
\]

a) Show that with these operations \( R \) becomes a ring. Is it commutative? Does it have an identity element?
b) Show that the set \( S = \{ (a, b) \in R \mid a, b \text{ even} \} \) is a subring.

16) Consider the set \( R = \left\{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \) of vectors. If we consider the usual addition and the cross product

\[
\begin{pmatrix} a \\ b \\ c \end{pmatrix} \times \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} bf - ec \\ dc - af \\ ae - bd \end{pmatrix}
\]

as multiplication, is this set a ring?

17) Which of the following sets are rings (with the usual addition and multiplication)? Do they have an identity?

1. The natural numbers;
2. real polynomials of degree at most \( n \);
3. polynomials with integer coefficients;
4. polynomials with integer coefficients and constant term zero;
5. polynomials with integer coefficients and degree at most four;
6. all real polynomials such that \( p(2) = 0 \);
7. all integers divisible by \( 3 \);
8. all non-singular \( 2 \times 2 \) matrices with real entries.

**Hint:** It might be easiest to show that a set is a subring of a larger ring.

18\*) Let \( R = \mathbb{Z} \). Define a new addition and a multiplication, that makes \( R \) a ring, but such that 0 is not the zero element of \( R \) and 1 not the one.

**Hint:** Consider \( a \oplus b = ((a - 3) + (b - 3)) + 3 \)

19) Show that the ring \( R \) of \( 2 \times 2 \) matrices with rational entries contains elements \( a, b \in R \) such that \( ab = 0 \) but \( ba \neq 0 \).

Problems marked with a * are bonus problems for extra credit.