Show your work. Bare answers will not be accepted, not even for partial credit. Passing grade is 50.

1. **Find the remainder when $37^{126}$ is divided by 13. (5 pts.)**  
   **Solution:** Since 
   $$(-2)^2 \equiv 4 \pmod{13}$$  
   $$(-2)^3 \equiv -8 \pmod{13}$$  
   $$(-2)^4 \equiv 16 \equiv 3 \pmod{13}$$  
   $$(-2)^5 \equiv -6 \pmod{13}$$  
   $$(-2)^6 \equiv 12 \equiv -1 \pmod{13}$$  
   $$(-2)^{12} \equiv (-1)^2 \equiv 1 \pmod{13},$$
   we have, $37^{126} \equiv (-2)^{126} \equiv (-2)^{12 \times 10 + 6} \equiv (-2)^{12} \times (-2)^{6} \equiv (-2)^6 \equiv -1 \equiv 12 \pmod{13}.$

2. **Show that** $1 + \sum_{i=0}^{n} (-2)^i \binom{n}{i} = (-1)^n.$ (5 pts.)  
   **Proof:** Since $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ for all $x$ and $y$, taking $x = -2$ and $y = 1$, we get the answer.

3. **Let $d$ be the greatest common divisor of the two positive integers $a$ and $b.$**
   **3a. Show that there are integers $x$ and $y$ such that $ax + by = d.$** (10 pts.)  
   **Proof:** We proceed by induction on $\max(a, b)$. If $a = b$ then we must have $d = a = b$ and in this case we take $x = 1$, $y = 0$ e.g. This takes care of the first step of the induction, since the condition “$\max(a, b) = 1$” is equivalent to the condition “$a = b = 1$”. Assume from now on that we know the result for $a', b'$ in case $\max(a', b') < \max(a, b)$. By the first part of the proof we may also assume that $a \neq b$. By symmetry we may further assume that $a > b$. (If that is not the case, exchange the roles of $a$ and $b$). Clearly $\gcd(a - b, b) = \gcd(a, b) = d$ (because any number that divides one of the pairs must divide the other pair.) Since $a - b < a$ and $b < a$, $\max(a - b, b) < a = \max(a, b)$, we may apply inductive hypothesis to find two integers $x'$ and $y'$ such that $(a - b)x' + by' = d$. Therefore $ax' + b(y' - x') = d$. Take $x = x'$ and $y = y' - x'$ to finish the proof.

3b. **Let $a = 23023$, $b = 24871.$ Find $d$, $x$ and $y$ as above.** (10 pts.)  
   **Answer:** This is the famous Euclid’s algorithm. We do the successive divisions:  
   
   \[
   \begin{align*}
   24871 &= 23023 \times 1 + 1848 \\
   23023 &= 1848 \times 12 + 847 \\
   1848 &= 847 \times 2 + 154 \\
   847 &= 154 \times 5 + 77 \\
   154 &= 77 \times 2 + 0 
   \end{align*}
   \]
   Therefore $d = 77$ (the remainder just before the 0 remainder). To find $x$ and $y$ we start from the before the last equation and go backwards:  
   $77 = 847 - 154 \times 5$
Therefore, we may take $x = 148$ and $y = -137$. (There may be other answers. As an exercise, given one pair $x$ and $y$ of solution find all the others in terms of $x$, $y$, $a$ and $b$.)

4. Let $aX^2 + bX + c \in \mathbb{Z}[X]$ have two distinct integer roots. Show that a must divide both $b$ and $c$. (10 pts.)

**Proof:** Let $\alpha, \beta \in \mathbb{Z}$ be the two roots of $aX^2 + bX + c$. Then $X - \alpha$ divides $aX^2 + bX + c$, say, $aX^2 + bX + c = (X - \alpha)(dX + e)$. Applying $\beta$ both sides, since $\alpha \neq \beta$, we get $d\beta + e = 0$. Thus $dX + e = dX - d\beta = d(X - \beta)$. Hence $aX^2 + bX + c = (X - \alpha)(dX + e) = d(X - \alpha)(X - \beta)$. It follows that $a = d$, $b = -d(\alpha + \beta)$, $c = d\alpha\beta$. This proves the statement.

5. Let $b, c \in \mathbb{Z}$. Show that the necessary and sufficient condition for the equation $x^2 + bx + c = 0$ to have a root in $\mathbb{Z}$ is that $b^2 - 4c$ is a perfect square in $\mathbb{Z}$. (10 pts.)

**Proof:** It is well-known that the roots in $\mathbb{Q}$ are given by the quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$ 

Thus the polynomial has a root in $\mathbb{Z}$ if and only if $b^2 - 4c$ is a perfect square in $\mathbb{Z}$ and if one of the two $-b \pm \sqrt{b^2 - 4c}$ is even. But if $b^2 - 4c$ is a perfect square in $\mathbb{Z}$, then it is easy to check that the numbers $-b \pm \sqrt{b^2 - 4c}$ are always even. Thus the polynomial has a root in $\mathbb{Z}$ if and only if $b^2 - 4c$ is a perfect square in $\mathbb{Z}$.

6. Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial (i.e. the leading coefficient of $f$ is 1). Show that all the rational roots of $f$ are integers. (10 pts.)

**Proof:** Let $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$. Let $r/s$ be a rational root of $f$ with $r, s \in \mathbb{Z}$. We may assume that $r$ and $s$ are prime to each other. We will show that $s = \pm 1$, proving that the root $r/s$ is an integer. Since $r/s$ is a root, we have $f(r/s) = 0$, i.e.,

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + ... + a_0 = 0.$$ 

By equalizing the denominator, we get,

$$r^n + a_{n-1}r^{n-1}s + ... + a_0s^{n-1} = 0.$$ 

Since $s$ divides all the terms except may be the first one, $s$ must also divide the first term. Thus $s$ divides $r^n$. Since $r$ and $s$ are prime to each other, this is possible only if $s = \pm 1$.

7. Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_0$ be a real polynomial with $a_n \neq 0$.

7a. Let $\alpha$ be a real root of $f$. Show that $|\alpha| \leq \sup \{1, |a_{n-1}/a_n| + ... + |a_0/a_n|\}$. (10 pts.)

**Proof:** If $|\alpha| \leq 1$ this is clear. Assume from now on that $|\alpha| \geq 1$. Since $f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$, we have,

$$\alpha^n = -(a_{n-1}/a_n)\alpha^{n-1} + (a_{n-2}/a_n)\alpha^{n-2} + ... + (a_0/a_n).$$ 

By taking the absolute values of both sides we get,

$$|\alpha|^n = |-(a_{n-1}/a_n)\alpha^{n-1} + (a_{n-2}/a_n)\alpha^{n-2} + ... + (a_0/a_n)|$$

$$\leq |a_{n-1}/a_n||\alpha|^{n-1} + |a_{n-2}/a_n||\alpha|^{n-2} + ... + |a_0/a_n|$$

$$\leq |a_{n-1}/a_n||\alpha|^{n-1} + |a_{n-2}/a_n||\alpha|^{n-2} + ... + |a_0/a_n||\alpha|^{n-1}$$
\[
= (|a_{n-1}/a_n| + |a_{n-2}/a_n| + ... + |a_0/a_n|)|\alpha|^{n-1}.
\]

Hence,
\[|\alpha| \leq |a_{n-1}/a_n| + |a_{n-2}/a_n| + ... + |a_0/a_n|.\]

**7b. Deduce that there is an algorithm for finding all the integer roots of a polynomial in \(\mathbb{Z}[X]\).** (5 pts.)

**Proof:** By 7a we need to check only finitely many integers.

**8. Let** \(f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]\) **be a polynomial with** \(a_n \neq 0\). Let \(\alpha\) **be a rational root of** \(f\). **Write** \(\alpha = r/s\) **with** \(r, s \in \mathbb{Z}\) **and** \(\gcd(r, s) = 1\).

**8a. Show that** \(s\) **divides** \(a_n\). **(10 pts.)**

**Proof:** This is similar to the solution of #6. Since \(f(r/s) = 0\), after equalizing the denominators, we get,
\[a_nr^n + a_{n-1}r^{n-1}s + ... + a_0s^n = 0.\]
Since \(s\) appears in all the terms except in the first one, \(s\) must divide the first term \(a_nr^n\). Since \(r\) and \(s\) are prime to each other, this implies that \(s\) divides \(a_n\).

**8b. Using #7a show that** \(|r| \leq \sup(|a_n|, |a_{n-1}| + ... + |a_0|)\). **(10 pts.)**

**Proof:** By 8a, \(|s| \leq |a_n|\). By 7a, \(|r/s| \leq \sup\{1, |a_{n-1}/a_n| + ... + |a_0/a_n|\}\), i.e.
\[|r| \leq |s| \sup\{1, |a_{n-1}/a_n| + ... + |a_0/a_n|\} \leq |a_n| \sup\{1, |a_{n-1}/a_n| + ... + |a_0/a_n|\} = \sup\{|a_n|, |a_{n-1}| + ... + |a_0|\}.
\]

**8c. Deduce that there is an algorithm for finding all the rational roots of a polynomial in \(\mathbb{Z}[X]\).** (5 pts.)

**Proof:** By 8a we need to try only finitely values for \(s\). By 8b we need to try only finitely values for \(r\). Thus we need to check only finitely many rationals.