Problem 1. (2 points.) Let \( f(x) = x^3 + ax + b \in \mathbb{Z}[x] \) be a cubic polynomial and let \( r_1, r_2, r_3 \in \mathbb{C} \) be the roots of 
\[
    f(x) = 0.
\]
If \( r_1 = r_2 \), then prove that \( r_1, r_2, r_3 \in \mathbb{Z} \).

Solution. We know that
\[
    r_1 + r_2 + r_3 = 0 \quad \text{and so, since } r_1 = r_2,
\]
\[
    r_3 = -2r_1.
\]
But also, we know that
\[
    r_1r_2 + r_1r_3 + r_2r_3 = a \quad \text{and thus}
\]
\[
    -3r_1^2 = a,
\]
which proves that \( r_1^2 \in \mathbb{Q} \). Finally, we know that
\[
    r_1r_2r_3 = -b \quad \text{and so, } -2r_1^3 = -b,
\]
thus proving that \( r_1^3 \in \mathbb{Q} \). In conclusion, \( r_1 \in \mathbb{Q} \) and so, also \( r_3 \in \mathbb{Q} \). However, any rational solution to a monic equation with integer coefficients must be an integer, i.e., if \( \frac{a}{b} \) (in lowest terms) is a root of the monic polynomial equation
\[
    x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0 = 0,
\]
where each \( c_i \) is an integer, then we would get that
\[
    a^d = - \sum_{i=0}^{d-1} c_i b^{d-i} a^i
\]
and so, if there exists a prime \( p \) dividing \( b \), then we would have that also \( p \mid a \), contradicting the fact that \( \frac{a}{b} \) is in lowest terms. Therefore, indeed, any rational root of a monic polynomial with integer coefficients must be an integer itself, thus proving that \( r_1, r_2, r_3 \in \mathbb{Z} \).

Problem 2. (1 point.) Let \( f(x) = x^3 + ax + b \in \mathbb{Z}[x] \) be a cubic polynomial and let \( r_1, r_2, r_3 \in \mathbb{C} \) be the roots of 
\[
    f(x) = 0.
\]
If \( r_1 = r_2 \), then prove that there exist infinitely many positive integers \( n \) such that \( f(n) \) is not a perfect square.

Solution. By Problem 1, we know that \( r_1 = r_2 =: r \) and \( r_3 =: s \) must be integers. So,
\[
    x^3 + ax + b = (x - r)^2 \cdot (x - s).
\]
Therefore, for any positive integer \( n \) such that \( n - s \) is not a perfect square, we also have that \( f(n) \) is not a perfect square.
Problem 3. (1 point) Let \( f(x) \in \mathbb{Z}[x] \), let \( n_0, \ell \in \mathbb{Z} \) and let \( p \) be a prime number. Assume the following:
- \( p \nmid \ell \); and
- \( p^2 \mid (f(n_0 + \ell p) - f(n_0)) \).
Then prove that \( p \mid f'(n_0) \) (where \( f'(x) \) is the derivative of the polynomial \( f(x) \)).

Solution. We let
\[
    f(x) = \sum_{i=0}^{d} c_i x^i
\]
and then expand
\[
    f(n_0 + \ell p) = f(n_0) + \ell p \cdot f'(n_0) + \sum_{i=2}^{d} c_i \cdot \sum_{j=2}^{i} (\ell^j) n_0^{i-j} \\
    \equiv f(n_0) + \ell p f'(n_0) \pmod{p^2}.
\]
So, if \( p^2 \mid f(n_0) \) and also \( p^2 \mid f(n_0 + \ell p) \), then we must have that \( p \mid f'(n_0) \) since \( p \nmid \ell \).

Problem 4. (4 points) Let \( f, g \in \mathbb{Z}[x] \) be polynomials with the property that there exists no \( r \in \mathbb{C} \) such that
\[
    f(r) = g(r) = 0.
\]
Then prove that there exists a nonzero integer \( m \) and there exist \( P, Q \in \mathbb{Z}[x] \) such that \( f(x) \cdot P(x) + g(x) \cdot Q(x) = m \).

Solution. We apply the Euclidean Algorithm in \( \mathbb{Q}[x] \), i.e., divide repeatedly the polynomials, recording the remainder each time. More precisely, assuming (without loss of generality) that \( \deg(f) \geq \deg(g) \), we write
\[
    f(x) = g(x) \cdot Q_1(x) + R_1(x) \quad \text{with} \quad \deg(R_1) < \deg(g).
\]
Then we write
\[
    g(x) = R_1(x) \cdot Q_2(x) + R_2(x) \quad \text{with} \quad \deg(R_2) < \deg(R_1)
\]
and then
\[
    R_1(x) = R_2(x) \cdot Q_3(x) + R_3(x) \quad \text{with} \quad \deg(R_3) < \deg(R_2).
\]
We continue until we are left with a remainder \( R_m(x) \) which is a constant polynomial (since the degrees of the polynomials \( R_i(x) \) decrease with \( i \)).

We claim that the first time when this happens (i.e., for the minimal such \( m \)) we have that \( R_m(x) \neq 0 \). Indeed, if \( R_m(x) = 0 \), then we would have that the polynomial \( R_{m-1}(x) \) must divide \( R_{m-2}(x) \) and furthermore (since \( m \) is minimal), \( R_{m-1}(x) \) is a nonconstant polynomial. Hence, there exists a root \( r \) of \( R_{m-1}(x) = 0 \) and clearly (since \( R_{m-2}(x) = Q_m(x) \cdot R_{m-1}(x) \)) we have that also \( R_{m-1} \) has the root \( r \). Arguing backwards, starting with the polynomials \( R_{m-1} \) and \( R_{m-2} \), which share the same root \( r \), we obtain that also \( R_{m-3} \) and in general, each \( R_i(x) \) has the root \( r \). In particular, \( g(x) \) and \( R_2(x) \) would share the root \( r \), which would then force also \( f(x) \) to have the root \( r \), contradicting the fact that \( f(x) \) and \( g(x) \) share no common root. Therefore, indeed, the first time when \( R_m(x) \) is a constant polynomial, we have that \( R_m(x) \neq 0 \).
We let \( c := R_m(x) \) (which is a constant in \( \mathbb{Q} \)) since all the polynomials \( Q_i(x) \) and \( R_i(x) \) have rational coefficients) and then note that

\[
c = 1 \cdot R_{m-1}(x) - Q_m(x) \cdot R_{m-2}(x).
\]

We continue solving backwards for the \( R_i(x) \) (exactly as we do in the usual Euclidean Algorithm when dealing with the greatest common divisor of integers) and therefore, we derive the existence of some polynomials \( P_0, Q_0 \in \mathbb{Q}[x] \) such that

\[
c = f(x)P_0(x) + g(x)Q_0(x).
\]

Finally, multiplying by some positive integer \( N \) to clear all the possible denominators in \( c \) and in each coefficient of \( P_0(x) \) and of \( Q_0(x) \), we obtain the existence of a nonzero integer \( m \) and also, the existence of two polynomials \( P \) and \( Q \) with integer coefficients such that

\[
f(x)P(x) + g(x)Q(x) = m.
\]

**Problem 5.** (4 points) Let \( f \in \mathbb{Z}[x] \) be a nonconstant polynomial. Prove that the set

\[
S = \{ p \text{ prime: there exist infinitely many positive integers } n \text{ such that } p \mid f(n) \}
\]

is infinite.

**Solution.** Let \( f(x) = \sum_{i=0}^{d} c_i x^i \). Clearly, if \( c_0 = 0 \), then for each prime \( p \) and for each \( k \in \mathbb{N} \), we have that \( f(pk) \) is divisible by \( p \) and therefore, each prime \( p \) is in the set \( S \). So, from now on, we assume \( c_1 \neq 0 \).

Assume the set \( S \) is finite. We let \( S_1 \) be the set of primes appearing in \( S \) along with the finitely many primes which may divide \( c_0 \) (if \( c_0 = \pm 1 \) then \( S_1 = S \)). We let

\[
P := \prod_{p \in S_1} p.
\]

If \( S_1 \) were empty, then we simply let \( P = 1 \).

Let \( N \) be a sufficiently large positive integer such that \( |f(x)| > 1 + |c_0| \) for all \( x \geq N \). Then

\[
f(NP|c_0|) = |c_0| \cdot \left( \epsilon_0 + P \cdot \sum_{i=1}^{d} c_i (P|c_0|)^{i-1} N^i \right),
\]

where \( \epsilon_0 := \frac{c_0}{|c_0|} \in \{-1, 1\} \). Since \( f(NP|c_0|) > 1 + |c_0| \) according to our hypothesis, we must have that the integer

\[
N_1 := \epsilon_0 + P \cdot \sum_{i=1}^{d} c_i (P|c_0|)^{i-1} N^i
\]

is an integer not equal to 0, 1 or \(-1\). So, there exists a prime \( q \) dividing \( N_1 \); furthermore this prime \( q \) does not divide \( P \) and so, it cannot be in the set \( S \). However, once we know that \( q \) divides \( N_1 \) and thus, \( q \mid f(NP|c_0|) \) we must also have that \( q \) divides \( f(NP|c_0| + q\ell) \) for any positive integer \( \ell \) (note that \( P(a) \equiv P(b) \) (mod \( q \)) if \( a \equiv b \) (mod \( q \))); so, \( q \) must belong to the set \( S \), contradiction. Therefore, indeed, \( S \) must be an infinite set.
Problem 6. (4 points.) Let \( f \in \mathbb{Z}[x] \) be a nonconstant polynomial with the property that all the roots (in \( \mathbb{C} \)) for the equation
\[
f(x) = 0
\]
are distinct. Prove that there exist infinitely many positive integers \( n \) such that \( f(n) \) is not a perfect square.

Solution. Assume the contrary and therefore, assume that there exists some positive integer \( N_0 \) such that for all \( n \geq N_0 \), we have that \( f(n) \) is a perfect square.

Since all the (complex) roots of \( f(x) \) are distinct, then \( f(x) \) and its derivative \( f'(x) \) share no common root. Then (since they are both polynomials with integer coefficients), Problem 4 yields the existence of a nonzero integer \( m \) and also, the existence of polynomials \( P, Q \in \mathbb{Z}[x] \) such that
\[
f(x)P(x) + f'(x)Q(x) = m.
\]
Now, we let \( S \) be the set from Problem 5 associated to \( f(x) \), i.e., the set of all primes dividing \( f(n) \) (for infinitely many) positive integers \( n \). Since we know now that \( S \) is infinite, we can choose a prime \( q \in S \) which does not divide the nonzero integer \( m \).

Now, let \( n_0 \geq N_0 \) be an integer such that \( q \mid f(n_0) \); in particular, because (by our assumption) \( f(n_0) \) is a perfect square, then we must have that \( q^2 \mid f(n_0) \). Now, for each \( \ell \in \mathbb{N} \), we have that
\[
f(n_0 + \ell q) \equiv f(n_0) \equiv 0 \pmod{q}
\]
and so, \( q \mid f(n_0 + \ell q) \) and since \( n_0 + \ell q > N_0 \), we get that also \( f(n_0 + \ell q) \) is a perfect square, which means that \( q^2 \mid f(n_0 + \ell q) \).

Using the conclusion of Problem 3 for \( \ell \) not divisible by \( q \), we obtain that \( q \mid f'(n_0) \). But then \( q \) divides \( f(n_0) \cdot P(n_0) + f'(n_0) \cdot Q(n_0) = m \), which is a contradiction. So, in conclusion, there must be infinitely many positive integers \( n \) such that \( f(n) \) is not a perfect square.

Problem 7. (1 point.) Let \( f(x) \in \mathbb{Z}[x] \) be a polynomial of degree 3. Prove that there exist infinitely many positive integers \( n \) such that \( f(n) \) is not a perfect square.

Solution. We deal with a cubic polynomial with integer coefficients:
\[
f(x) = ax^3 + bx^2 + cx + d, \text{ where } a \neq 0.
\]
If \( a < 0 \) then \( \lim_{n \to \infty} f(n) = -\infty \) and so, clearly, there exist infinitely many positive integers \( n \) such that \( f(n) \) is not a perfect square. So, from now on, we assume \( a > 0 \).

By Problem 6, we know that if all roots of \( f(x) \) are distinct, then we are done. So, from now on, we assume there exists a double root \( r \) for \( f(x) \). Immediately this proves that all roots of \( f(x) \) are rational (with the proof essentially as for Problem 1). Indeed, we argue using linear transformations to modify the above cubic polynomial into a cubic polynomial of the form \( a^3 + Ax + B \). In order to do this, we note that solving \( f(x) = 0 \) is equivalent with solving \( 27a^2f(x) = 0 \), i.e.,
\[
(3ax)^3 + 3b(3ax)^2 + 9ca(3ax) + 27da^2 = 0
\]
and so, it suffices to prove that the roots of
\[
x^3 + 3bx^2 + 9cax + 27da^2 = 0
\]
are rational. This yields the equation:

\[(x + b)^3 + (9ca - 3b^2)(x + b) + 27da^2 + 2b^3 - 9abc = 0,\]

and therefore, the roots of \(f(x) = 0\) are rational if and only if the roots of

\[x^3 + Ax + B = 0\]

are rational, where \(A = 9ca - 3b^2\) and \(B = 27da^2 + 2b^3 - 9abc\); furthermore, since we can navigate between the two equations through the above linear transformations, once we know that the original equation has a double root, then also the equation

\[x^3 + Ax + B = 0\]

has a double root and therefore, by Problem 1, all the roots of \(f(x) = 0\) are rational (we can no longer guarantee that they are integral since the above linear transformations performed in reverse order may introduce denominators even though we know we start with some integral solutions to the equation \(x^3 + Ax + B = 0\)).

So, we know that \(f(x) = a(x - r)^2(x - s)\). We write \(s := \frac{N}{D}\) for some coprime integers \(D\). Pick a prime \(p > \max\{|a|, |N|, |D|\}\) and then let \(n_0 \in \mathbb{N}\) such that

\[n_0D \equiv N \pmod{p},\]

which is possible since \(D\) is invertible modulo \(p\). Then for each \(\ell \in \mathbb{N}\), the exponent of the prime \(p\) in \(f(n_0 + \ell p)\) has the same parity as the exponent of the prime \(p\) in \(nD - N\) and therefore, since

\[p \mid (n_0 + \ell p)D - N,\]

then for each prime \(\ell\) such that \(f(n_0 + \ell p)\) is a perfect square, we must have that

\[\exp_p((n_0 + \ell p)D - N) \geq 2.\]

But the difference between any two consecutive integers in the arithmetic progressions \(\{(n_0 + \ell p)D - N\}_{\ell \in \mathbb{N}}\) is \(pD\), while the difference between multiples of \(p^2\) is at least \(p^2\), contradiction. So, indeed, there must be infinitely many \(n\) such that \(f(n)\) is not a perfect square.

**Problem 8.** (8 points.) Let \(f(x) = x^3 + 23\). Find all integers \(n\) with the property that \(f(n)\) is a perfect square.

**Solution.** Let \(n\) be a positive integer such that \(f(n) = m^2\) for some nonnegative integer \(m\). So, we have

\[m^2 = n^3 + 27\]

and analyzing this diophantine equation modulo 4, we get two cases.

**Case 1.** \(n\) is even.

In this Case 1, we have that \(n^3 \equiv 0 \pmod{8}\) and so,

\[m^2 \equiv n^3 + 27 \equiv 3 \pmod{8},\]

which is impossible. Therefore, we must have only

**Case 2.** \(n\) is odd.

In this Case 2, we get that \(m^2\) and therefore \(m\) itself must be even (since \(n^3 + 27\) is even in this Case 2). So,

\[n^3 + 27 \equiv m^2 \equiv 0 \pmod{4},\]
which yields that $n^3 \equiv 1 \pmod{4}$. Since already we have that $n^2 \equiv 1 \pmod{4}$ (because $n$ is odd) then we must have that $n$ itself is 1 modulo 4.

We also have

$$m^2 + 4 = n^3 + 27 = (n + 3)(n^2 - 3n + 9)$$

and since $n \equiv -1 \pmod{4}$, we get that

$$n^2 - 3n + 9 \equiv -1 \pmod{4}.$$ 

On the other hand, for any positive integer $n$, we have that

$$n^2 - 3n + 9 = \left( n - \frac{3}{2} \right)^2 + \frac{27}{4} > 6.$$ 

So, the number $n^2 - 3n + 9$ is greater than 6 and it is $-1$ modulo 4; therefore, it must be divisible by some prime $q$ which is itself $-1$ modulo 4. But then this prime number $q$ must also divide $n^2 + 4$, which is impossible since this would mean that $-4$ (and therefore $-1$) is a quadratic residue modulo $q$ (which contradicts the fact that $q \equiv -1 \pmod{4}$). In conclusion, there exists no positive integer $n$ such that $f(n)$ is a perfect square.