Problem 4. Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial with integral coefficients. Suppose that there are $n \geq 5$ consecutive integers at which the value of f is a perfect square. Prove that $b^2 - 4ac$ is divisible by every prime number smaller or equal than n.

Solution. Before we start let us make the following simple observation: for any integer m the function $g(x) = f(x - m)$ is of the form $g(x) = ax^2 + b_1x + c_1$ and $b^2 - 4ac = b_1^2 - 4ac_1$. This allows us, when convenient, to assume that $f(0), \ldots, f(n-1)$ are squares (by choosing suitable m).

Let us start by showing that $b^2 - 4ac$ is divisible by 2 if the value of f at three consecutive integers is a square. Showing that $b^2 - 4ac$ is divisible by 2 is equivalent to showing that b is even. Suppose that $f(m-1) = l^2$, $f(m)$, and $f(m+1) = k^2$ are squares for some integer m. Note that $k^2 - l^2 = f(m+1) - f(m-1) = 4am + 2b$ is even. It follows that k, l have the same parity and therefore $k^2 - l^2 = (k-l)(k+l)$ is divisible by 4 (as a product of two even integers). Thus $4am + 2b$ is divisible by 4, and therefore b is even (note that we did not use the fact that $f(m)$ is a square).

Remark. The essence of the above argument is the simple but important observation that the square of an integer is congruent to 0 or 1 modulo 4.

Let now p be an odd prime number. We will be working with residues modulo p (i.e. congruences modulo p). We say that an integer m is (is not) a **square modulo** p if m is (is not) congruent to a square of an integer modulo p. For example, -1 is a square modulo 5 but 2 is not a square modulo 5. It is clear that being a square modulo p depends only on the residue class modulo p, i.e. two numbers congruent modulo p are either both squares modulo p or both are non-squares modulo p.

The key observation needed for our solution is the following result.

Proposition 1 *Among the numbers $0, 1, ..., p-1$ exactly $(p+1)/2$ are squares modulo p.*

Indeed, it is easy to see that no two among the numbers $0^2, 1^2, \ldots, [(p-1)/2]^2$ are congruent modulo p, so their residues modulo p form a set $(p+1)/2$ elements among $0, 1, ..., p-1$ which are squares modulo p. On the other hand, any integer m is congruent modulo p to $\pm j$ for some $j \in \{0, 1, \ldots, (p-1)/2\}$ and therefore $m^2 \equiv j^2 \pmod{p}$.

As a simple corollary we get the following result.

Proposition 2 *If p divides a and p does not divide b then $f(x)$ can be a square for at most $(p+1)/2$ consecutive integers x.*

Indeed, note that when p divides a then $f(m) \equiv bm + c \pmod{p}$ for every m. If $bk + c \equiv bl + c \pmod{p}$ then p divides $b(k-l)$, hence p divides $k - l$ (recall that p does not divide b). It follows that for any integer k, no two of the $1 + (p+1)/2$ numbers $bk + c, b(k+1) + c, \ldots, b(k + (p + 1/2)) + c$ are congruent modulo p, so at least one of them is not a square modulo p by Proposition 1.

Returning to the assumptions of the problem, we conclude immediately from Proposition 2 that if p is a prime which divides a and such that $p < 2n-1$, then p also divides b, and consequently $p|(b^2 - 4ac)$. This establishes the conclusion of the problem for primes which divide a. As a matter of fact it establishes more, that any prime $p < 2n - 1$ which divides a must divide $b^2 - 4ac$. We will use this in our second solution.

From now on we assume that p does not divide a and that $f(0), \ldots, f(n-1)$ are squares. Note that if k, l are integers then $f(k) - f(l) = (k-l)(a(k+l) + b)$. It follows that $f(k) \equiv f(l) \pmod{p}$ if and only if either $l \equiv k \pmod{p}$ or $l \equiv r - k \pmod{p}$, where

$$r \text{ is the unique integer in } \{0, 1, \ldots, p-1\} \text{ such that } ar \equiv -b \pmod{p}.$$

In particular, we see that among the numbers $f(0), f(1), \ldots, f(p-1)$ no three are congruent to each other modulo p.

Suppose now that $p \leq n$. Thus each of the p numbers $f(0), f(1), \ldots, f(p-1)$ is a square modulo p, and therefore $f(m)$ is a square modulo p for every integer m (see the observations in the previous paragraph). Recall now that from Proposition 1 we have exactly $(p+1)/2$ non-congruent squares modulo p. Our observations so far can be formulated as follows: we are distributing p pigeons (the squares $f(0), f(1), \ldots, f(p-1)$) into $(p+1)/2$ drawers (the congruence classes of squares modulo p) in such a way that each drawer has at most two pigeons. It follows that no drawer can be empty. In particular, we must have $f(i) \equiv 0^2 = 0 \pmod p$ for some $i \in \{0, 1, \ldots, p-1\}$. Choose smallest such i. Let j be an integer in $\{0, 1, \ldots, p-1\}$ such that $j \equiv r - i \pmod p$ (r was defined in the previous paragraph). Then $f(i) \equiv f(j) \pmod p$, so p divides $f(j)$ and therefore $j \geq i$.

If $j = i$ then $2i \equiv r \pmod p$ and therefore $2ai + b$ is divisible by p (by the definition of r). Now $(2ai+b)^2 - 4af(i) = b^2 - 4ac$, so $b^2 - 4ac$ is divisible by p^2 (note that since p divides $f(i)$ and $f(i)$ is a square, p^2 divides $f(i)$). Thus the conclusion of the problem holds in this case.

Suppose now that $j > i$. We will show that this is not possible unless $p = 3$. Set $k = j - i$ and $g(x) = ax(x-k)$ (note that $0 < k < p$). We claim than $g(m) \equiv f(m+i) \pmod p$ for every integer m. In fact, on one hand we have

$$g(m) = am(m-k) = am(m+i-j) \equiv am(m+i-(r-i)) = m(a(m+2i)-ar) \equiv m(a(m+2i)+b) \pmod p.$$

On the other hand,

$$f(m+i) \equiv f(m+i) - f(i) = m(a(m+2i)+b) \pmod p.$$

Thus $g(m) \equiv f(m+i) \pmod p$. It follows that $g(m)$ is a square modulo p for every integer m. Suppose now that p does not divide w. There is an integer m such that $mw \equiv 1 \pmod p$. Then

$$w^2 g(m) = amw(wm - kw) \equiv a(1-kw) \pmod p.$$

Thus $a(1-kw)$ is a square modulo p for every w not divisible by p. Note that no two of the numbers $a(1-k), a(1-2k), \ldots, a(1-(p-1)k)$ are congruent modulo p. Thus we have $p-1$ pairwise non-congruent squares modulo p. This means that $p - 1 \leq (p+1)/2$, i.e. $p \leq 3$.

It remains to consider the case when $p = 3$, $f(0), f(1), f(2), f(3), f(4)$ are squares and p divides $f(i)$ and $f(j)$ for some $0 \leq i < j < 3$. Thus $i \leq 1$ and both $f(i)$ and $f(i+3)$ are squares divisible by 3, hence also divisible by 9. Now $f(i+3) - f(i) = 3(a(2i+3)+b)$. Thus 3 divides $a(2i+3)+b$, so 3 divides $2ai+b$. Now $b^2 - 4ac = (2ai+b)^2 - 4af(i)$ is divisible by 3 (in fact by 9), as required to prove. This completes our argument.

Remark. Consider the polynomial $f(x) = 8x^2 - 8x + 9$. Then $b^2 - 4ac = -2^5 \cdot 7$ is not divisible by 3 and $f(-1) = 25, f(0) = 9, f(1) = 9, f(2) = 25$ are squares. Thus $n \geq 5$ is necessary to get divisibility by 3.

Remark. The above solution was intentionally written using just the basic properties of congruences. While this makes the argument very "elementary", the price to pay is that some parts of the reasoning may seem mysterious. Readers familiar with a bit more algebra should rewrite the proof using the fact that the residues modulo p form a field and then using the basic properties of polynomials over a field (like the fact that a polynomial of degree d assumes a given value in at most d different arguments, etc.). In particular, the fact that p divides $b^2 - 4ac$ says that the polynomial f modulo p has discriminant 0 and therefore a double root.

Second solution. We will prove now a stronger result that when $n \geq 5$ then $b^2 - 4ac$ is divisible by every prime number $p \leq 2n - 5$, using a bit more of elementary number theory (all we need is covered in a basic number theory class like Math 407 at Binghamton University). For $p \leq 3$ or when p divides a our argument is as in the first solution. So we assume that $p \geq 5$ and a is not divisible by p.

First we state some results and concepts we will need. For an odd prime p and any integers m we define the Legendre symbol $\left(\dfrac{m}{p}\right)$ as follows:

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } m \\ 1 & \text{if } m \text{ is a square modulo } p \text{ not divisible by } p \\ -1 & \text{if } m \text{ is not a square modulo } p. \end{cases}$$

Recall now the Fermat's Little Theorem:

If p does not divide m then $m^{p-1} \equiv 1 \pmod{p}$.

It follows that $m^{(p-1)/2} \equiv \pm 1 \pmod{p}$ for every integer m not divisible by p (since ± 1 are the only solutions of the congruence $x^2 \equiv 1 \pmod{p}$). If $m \equiv k^2 \pmod{p}$ for some k and p does not divide m then $m^{(p-1)/2} \equiv k^{p-1} \equiv 1 \pmod{p}$. On the other hand, if m is not a square modulo p then $m^{(p-1)/2} \not\equiv 1 \pmod{p}$ (this follows from the fact that the congruence $x^{(p-1)/2} \equiv 1 \pmod{p}$ has at most $(p-1)/2$ solutions). It follows that $m^{(p-1)/2} \equiv -1 \pmod{p}$ when m is not a square modulo p. We can summarize these observations as follows:

$$\left(\frac{m}{p}\right) \equiv m^{(p-1)/2} \pmod{p}$$

for every integer p. This observation is often called *Euler's criterion.* It is a simple exercise to derive from the Euler's criterion that

$$\left(\frac{mk}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{k}{p}\right)$$

for any integers m, k.

Let $S_k = \sum_{i=0}^{p-1} i^k$. Then

$$S_k \equiv \begin{cases} 0 \pmod{p} & \text{if } 0 \le k \le p-2 \\ -1 \pmod{p} & \text{if } k = p-1. \end{cases} \tag{1}$$

The case when $k = p-1$ is a straightforward corollary from Fermat's Little Theorem. To justify this when $0 \le k \le p-2$ note that for any u not divisible by p we have

$$u^k S_k = \sum_{i=0}^{p-1} (ui)^k \equiv \sum_{i=0}^{p-1} i^k = S_k \pmod{p}.$$

In other words, p divides $(u^k - 1)S_k$. Since the congruence $x^k \equiv 1 \pmod{p}$ has at most k solutions modulo p,there is u such that p does not divide any of u and $u^k - 1$ and using such u we conclude that p divides S_k.

We are ready to prove our claim. Using Euler's criterion we see that

$$\sum_{i=0}^{p-1} \left(\frac{f(i)}{p}\right) \equiv \sum_{i=0}^{p-1} f(i)^{(p-1)/2} \pmod{p}.$$

Now $f(x)^{(p-1)/2} = a^{(p-1)/2}x^{p-1} + h_{p-2}x^{p-2} + \ldots + h_1 x + h_0$ for some integers $h_0, h_1, \ldots, h_{p-2}$. By (1) and the Euler's criterion, we have

$$\sum_{i=0}^{p-1} f(i)^{(p-1)/2} \equiv a^{(p-1)/2} S_{p-1} + \sum_{j=0}^{p-2} h_j S_j \equiv -\left(\frac{a}{p}\right) \pmod{p}.$$

We see that

$$\sum_{i=0}^{p-1} \left(\frac{f(i)}{p}\right) \equiv -\left(\frac{a}{p}\right) = \pm 1 \pmod{p}.$$

Each summand on the left hand side is $-1, 0$ or 1. If we have s summands equal to 1, t summands equal to -1, and z summands equal to 0 then

$$z \le 2, \quad s + t + z = p, \quad \text{and} \quad s - t \equiv \pm 1 \pmod{p}.$$

Note that if $t > 0$ (i.e. $s + z < p$) then $n \le s + z$. To justify this recall from our first solution that we may assume that $f(0), \ldots, f(n-1)$ are squares. If $n > s + z$, then the $s + z + 1$ values $f(0), \ldots, f(s+z)$ would be squares modulo p. Thus for $0 \le i < p$ the Legendre symbol $\left(\frac{f(i)}{p}\right)$ can be -1 only when $p > i > s + z$. Since t is the number of $i \in \{0, 1, \ldots, p-1\}$ such that $\left(\frac{f(i)}{p}\right) = -1$, we see that $t < p - (s + z)$, which contradicts the equality $s + t + z = p$.

Since $-p \leq s-t \leq p$, we have $s-t=\pm 1$ or $s-t=\pm(p-1)$. Is $s-t=\pm(p-1)$ then s and t have the same parity, so $s+t$ is even and z must be odd. It follows that $z=1$. Thus there is exactly one $i \in \{0,1,\ldots,p-1\}$ such that $f(i)$ is divisible by p. As we have seen in our first solution, this means that $p|b^2-4ac$ (the polynomial $f(x)$ modulo p has a double root).

If $s-t=1$ then $2s-1+z=p$, so $2(s+z)=p+1+z \leq p+3$, i.e. $s+z \leq (p+3)/2$. It follows that $n \leq s+z \leq (p+3)/2$, i.e. $p \geq 2n-3$. If $s-t=-1$ then $2s+1+z=p$ and $n \leq s+z \leq (p+1)/2$, i.e. $p \geq 2n-1$. The last two cases contradict the assumption that $p \leq 2n-5$. This completes our argument.

Exercise. Show that if a prime p does not divide a and $p \leq n$ then p^2 divides b^2-4ac.

Example. Let $f(x)=84x^2-252x+289$. Then $b^2-4ac=-2^6\cdot 3\cdot 5^2\cdot 7$ and $f(x)$ is a square for $x=-1,0,1,2,3,4$ (so $n=6$).

Example (Provided by Dr. Mathew Wolak). Let $f(x)=-420x^2+2940x+289$. Then $f(x)$ is a square for $x=0,1,2,3,4,5,6,7$ (so $n=8$). Note that $b^2-4ac=2^5\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 19$.

Exercise. Show that if $p=2n-3$ is a prime which does not divide a and a is a square modulo p then p divides b^2-4ac. How does this explain why 13 shows up in the above example?

As far as we know the following are open problems.

Problem. Prove that there is k such that no quadratic polynomial $f(x)=ax^2+bx+c$ with integer coefficients such that $b^2-4ac\neq 0$ can assume square values at k consecutive integers. Find smallest such k.

Problem. Is there a monic polynomial $f(x)=x^2+bx+c$ with integer coefficients such that $b^2-4c\neq 0$ which assumes square values at 5 consecutive integers?

It is a result due to Fermat that there are no four distinct perfect squares which form an arithmetic progression. This is equivalent to the fact that no linear polynomial $bx+c$ with integer coefficients and $b\neq 0$ can assume square values at four consecutive integers.

To learn more about the concepts used in the above solutions one should consult any of the many books on elementary number theory. For example,

Elementary Number Theory by James K. Strayer

or (for more advanced treatment)

A classical Introduction to Modern Number Theory by Kenneth Ireland, Michael Rosen

are good choices.