Polynomial equations: from local solutions to global solutions

We prove the following result : for any distinct primes a, b such that

1. a is a square modulo b, and b is a square modulo a
2. At least one of a, b, ab is 1 modulo 8

Then the polynomial $P = (X^2 - a)(X^2 - b)(X^2 - ab)$ has a root in every finite ring (with 1), and (obviously) no root in $\mathbf{Z}$.
First we reduce the problem to specific rings: let R be a ring, let $f : \mathbf{Z} \to R$ be the unique ring morphism, then $\mathbf{Z}/\mathrm{Ker}f$ is isomorphic to a subring of R and so if P has a root in $\mathbf{Z}/\mathrm{Ker}f$, it has one in R as well.
Knowing the structure of ideals of $\mathbf{Z}$, it suffices to show that P has a root in $\mathbf{Z}/n\mathbf{Z}, n \geq 1$.
Moreover it is clear that P has a root in $\prod_{i \in I} R_i$ if and only if P has a root in each R_i; so the chinese remainder theorem allows us to reduce the problem to the following: prove that P has a root in each $\mathbf{Z}/p^\alpha\mathbf{Z}$, p a prime number and $\alpha \geq 0$.
That's where our hypotheses will be useful. We begin with the $p = 2$ case:

Lemma 1. *P has a root in $\mathbf{Z}/2^n\mathbf{Z}$, $n \geq 0$*

Proof. It suffices to find a square root to a, b or ab modulo 2^n. The second hypothesis yields such a root modulo 8 and so modulo $1, 2, 4$ as well.
We now wish to show that if $x \in \mathbf{Z}$ is 1 modulo 8, then it's a square modulo 2^n for each $n \geq 3$, from which the lemma will follow. Let $n \geq 3$
Let C_n denote the group of squares of invertible elements of $\mathbf{Z}/2^n\mathbf{Z}$, i.e. $C_n = \{x^2 \mid x \in (\mathbf{Z}/2^n\mathbf{Z})^\times\}$, and let $c_n : (\mathbf{Z}/2^n\mathbf{Z})^\times \to C_n$ be the squaring morphism. Letting $\pi^n : (\mathbf{Z}/2^n\mathbf{Z})^\times \to (\mathbf{Z}/8\mathbf{Z})^\times$ denote the canonical projection, we have $\pi^n_{|C_n} \circ c_n = c_3 \circ \pi^n$. As $C_3 = \{1\}$, we get $C_n \subset \mathrm{Ker}\pi^n$.
It's now just a matter of computing the respective orders of these subgroups: indeed assume we can prove they have the same order. Then they are equal, and so if $x \in \mathbf{Z}$ is 1 mod 8, then its reduction mod 2^n will be in $\mathrm{Ker}\pi$, hence in C_n, which is what we wanted.
π^n is surjective hence by the first isomorphism theorem $|\mathrm{Ker}\pi^n| = \frac{|(\mathbf{Z}/2^n\mathbf{Z})^\times|}{(\mathbf{Z}/8\mathbf{Z})^\times} = \frac{2^{n-1}}{2^{3-1}} = 2^{n-3}$.
But also $c_n : (\mathbf{Z}/2^n\mathbf{Z})^\times \to C_n$ is surjective and its kernel is has size 4 : indeed if $x^2 = 1 \bmod 2^n$ then $2^n \mid (x-1)(x+1)$. Letting α, β denote the respective 2-valuations of $x-1, x+1$ we have $\alpha + \beta \geq n$ but also there are some odd k, k' such that $2^\alpha k + 2 = 2^\beta k'$, so that $\min(\alpha, \beta) \leq 1$, hence $x = 1, -1, 2^{n-1} + 1$ or $2^{n-1} - 1 \bmod 2^n$. Hence $|C_n| = \frac{2^{n-1}}{4} = 2^{n-3}$. We are done for $p = 2$. □

There are three other cases : $p = a, b$ and $p \neq 2, a, b$. The cases $p = a$ and $p = b$ are essentially identical, we only deal with $p = a$.

Lemma 2. *P has a root in $\mathbf{Z}/a^n\mathbf{Z}$, $n \geq 0$*

Proof. If $a = 2$, lemma 1 suffices.
Otherwise by hypothesis 1, $Q = X^2 - b$ has a root in $\mathbf{Z}/a\mathbf{Z}$. Then we may lift this root mod a^n by Hensel's lemma: $Q' = 2X$ and so if r is root of Q, $2r$ is not 0 mod a (because otherwise b would be too, but $b \neq a$; and because a is odd). □

Of course the same proof works for an odd p, as long as we have a root mod p; hence it suffices to find a root of P mod p for p an odd prime $\neq a, b$.
This follows from the cyclicity of $(\mathbf{Z}/p\mathbf{Z})^\times$ and the following lemma:

Lemma 3. *Let $G = \langle\sigma\rangle$ be a cyclic group (denoted multiplicatively), and $x, y \in G$. Then at least one of x, y, xy is a square in G.*

Proof. Write $x = \sigma^n, y = \sigma^m$. If n or m is even then x or y is a square.
Otherwise, n, m are odd and so $n + m$ is even so that $xy = \sigma^{n+m}$ is a square. □

We thuse get a root of P mod p, and may lift it to $\mathbf{Z}/p^n\mathbf{Z}$ with Hensel's lemma, as in lemma 2. Thus we have a root in every $\mathbf{Z}/p^n\mathbf{Z}$, and so in every finite ring. There is obviously no root in $\mathbf{Z}$.

Remark 1. One may have trouble finding such a, b at first. Note for instance that lemma 3 cannot help for condition 2; as $(\mathbf{Z}/8\mathbf{Z})^\times$ is not cyclic ! I myself wondered if by any (bad) luck there weren't any such a, b. However, if I'm not mistaken, 5 and 61 work: 61 is 1 mod 5 so it's indeed a square and 5 is 26^2 mod 61; and finally $5 \times 61 = 305 = 1$ mod 8. I am told by a friend that $2, 17$ work as well: indeed $2 = 36$ mod $17 = 1$ mod 2 and $17 = 1$ mod 8.
Let me just note the following: if a is a prime that is 1 mod 8, and if, say c is an invertible square mod a; then by Dirichlet's theorem there will be infinitely many primes b that are c mod a, so that are squares mod a. For how many of those will a be a square mod b ?

Remark 2. One may prove lemma 2 in a more elementary fashion, without resorting to Hensel's lemma. The proof is very close to that of lemma 1. I wrote down the proof after the remarks, though it's not necessary.

Remark 3. Note that if we don't care about our polynomials being monic, then an easy example of a polynomial having a root in every finite ring and not in $\mathbf{Z}$ is $P = (2X-1)(3X-1)$ (a minimal example): the proof is easy and left as an exercise (hint : do the same sketch up to the $\mathbf{Z}/p^n\mathbf{Z}$, then wonder why 2 and 3). Here we found a *monic* polynomial, which may seem more "impressive".

Lemma 4. *Let p be an odd prime and a a square mod p. Then a is a square mod p^n for all $n \geq 0$*

Proof. Let $C_n(p)$ be the subgroup of invertible squares in $\mathbf{Z}/p^n\mathbf{Z}$, and let $c_n(p)$ be the squaring map $(\mathbf{Z}/p^n\mathbf{Z})^\times \to C_n(p)$.
Let $x \in \mathrm{Ker} c_n(p)$. Then $p^n \mid (x-1)(x+1)$. Let α, β be the p-valuations of $x-1$ and $x+1$ respectively. We have $\alpha + \beta \geq n$. But also for some k, k', $p^\alpha k + 2 = p^\beta k'$.
Say for instance $\alpha \geq \beta$, then $p^\beta(k' - p^{\alpha-\beta}k) = 2$. p is odd, so $\beta = 0$. A similar thing happens if $\alpha \leq \beta$: in any case $\min\{\alpha, \beta\} = 0$. Hence $\max\{\alpha, \beta\} \geq n$ and thus $x = 1$ or -1 mod p^n. This is a huge difference with $p = 2$, and explains why we need an 8 for this case.

There are thus $\frac{p-1}{2}p^{n-1}$ squares in $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

We have the same identity as before : $\pi^n_{|C_n(p)} \circ c_n = c_1 \circ \pi^n$, where $\pi^n : (\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ is the canonical projection; which is surjective $C_n(p) \to C_1(p)$. We thus have $|\mathrm{Ker}\pi^n \cap C_n(p)| = |\mathrm{Ker}\pi^n_{|C_n(p)}| = p^{n-1}$ and $|\mathrm{Ker}\pi^n| = p^{n-1}$, this last identity coming from the surjectivity of $\pi^n : (\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$; hence $\mathrm{Ker}\pi \subset C_n(p)$ and so if $\pi^n(x) \in C_1(p)$, $x \in C_n(p)$.
This clearly implies the lemma. □