HENSEL'S LEMMA AND SQUARES MOD N

TIM SMITS

For a prime p and and integer a co-prime to p, the value of the Legendre symbol $\left(\frac{a}{p}\right)$ detects whether or not a is a square mod p or not. For an odd integer $n = p_1^{e_1} \cdots p_k^{e_k}$, the Jacobi symbol $\left(\frac{a}{n}\right)$ generalizes the Legendre symbol, but the value of $\left(\frac{a}{n}\right)$ does *not* detect whether or not a is a square mod n or not: $\left(\frac{2}{15}\right) = 1$, yet 2 is not a square mod 15. How then, can one detect whether or not a is square mod n?

The guiding philosophy of number theory is the idea that information mod n is "the same" as information mod $p_i^{e_i}$, because one should be able to "glue" these pieces of information together using the Chinese remainder theorem. However, there is a second, equally as important philosophy: information mod p^e should come from "lifting" information mod p. One of the many instances of this philosophy is made precise in *Hensel's lemma*:

Theorem 0.1 (Hensel's lemma)**.** *Let $f(x)$ be a polynomial with integer coefficients, let p be a prime. Suppose that $f(c) \equiv 0 \bmod p$ for some c. If $f'(c) \not\equiv 0 \bmod p$, then for any $k \geq 1$ there exists an integer c_k such that $c_k \equiv c \bmod p$ and $f(c_k) \equiv 0 \bmod p^k$.*

The condition $f'(c) \not\equiv 0 \bmod p$ means that c is not a repeated root of the polynomial $f(x) \bmod p$. In this case, Hensel's lemma says we can "lift" the root to a root modulo any larger prime power. The proof of Hensel's lemma will rely on little more than basic calculus. Recall that for any $a \in \mathbb{R}$, the n-th Taylor polynomial of $f(x)$ centered at a is given by $T_n(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$. Since $f(x)$ is a polynomial of degree n, the n-th degree Taylor polynomial is actually *equal* to $f(x)$, so we have $f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$. Replacing x with $x+h$ and expanding around $a = x$, we may alternatively write this as $f(x+h) = \sum_{k=0}^{n} \frac{f^{(k)}(x)}{k!}h^k$.

Proof of Theorem 0.1. Our proof is by induction. For $k = 1$, the theorem is true by assumption. Now suppose that for some k there is an integer c_k with $c_k \equiv c \bmod p$ and $f(c_k) \equiv 0 \bmod p^k$. We will construct a solution to the congruence mod p^{k+1}. Specifically, consider an integer of the form $c_k + tp^k$ for some integer t. We would like to show that we can choose t such that $f(c_k + tp^k) \equiv 0 \bmod p^{k+1}$, as we may then take $c_{k+1} = c_k + tp^k$, and certainly we will have $c_{k+1} \equiv c_k \equiv c \bmod p$ as desired. Using a Taylor expansion, we may write $f(c_k + tp^k) = f(c_k) + f'(c_k)tp^k + \frac{f''(c_k)}{2}t^2p^{2k} + \ldots \equiv f(c_k) + f'(c_k)tp^k \bmod p^{k+1}$. Since $f(c_k) \equiv 0 \bmod p^k$, write $f(c_k) = p^k\ell$ for some $\ell \in \mathbb{Z}$. Then $f(c_k) + f'(c_k)tp^k = (\ell + f'(c_k)t)p^k$. If we can choose t to make the term in parenthesis divisble by p, we're done. Since $c_k \equiv c \bmod p$, we have $f'(c_k) \equiv f'(c) \not\equiv 0 \bmod p$, so the equation $\ell + tf'(c_k) \equiv 0 \bmod p$ has solution $t \equiv -\ell[f'(c)]^{-1} \bmod p$. Therefore, we may let t be any representative of this congruence class, and by construction this choice of t works. By induction, we're therefore done. □

Corollary 0.2. *Let p be an odd prime. An integer a co-prime to p is a square mod p if and only if a is a square mod p^k for all $k \geq 1$.*

Proof. First, suppose that $a \equiv c_k^2 \bmod p^k$ for $k \geq 1$. Then clearly $a \equiv c_k^2 \bmod p$, so a is a square mod p. Conversely, suppose that $a \equiv c^2 \bmod p$. With $f(x) = x^2 - a$, this means $f(c) \equiv 0 \bmod p$. Since $a \not\equiv 0 \bmod p$ we have $c \not\equiv 0 \bmod p$, and because p is odd we have $f'(c) = 2c \not\equiv 0 \bmod p$. By Hensel's lemma, for any $k \geq 1$ there is c_k such that $f(c_k) \equiv 0 \bmod p^k$, i.e. $a \equiv c_k^2 \bmod p^k$. □

The proof of Hensel's lemma is constructive, so it actually tells us how to *find* the square roots of a mod p^k!

Example 0.3. We have $2 \equiv 3^2 \bmod 7$, so Hensel's lemma tells us that 2 is a square mod 49. What are the solutions to $x^2 \equiv 2 \bmod 49$? Hensel's lemma says we want to take $3+7t$ where $t \equiv -\frac{f(3)}{7}[f'(3)]^{-1} \bmod 7$. We have $f(3) = 7$, $f'(3) = 6$, and $6^{-1} \equiv 6 \bmod 7$. Therefore, any choice of t with $t \equiv -6 \equiv 1 \bmod 7$ will work. Thus, $3+7\cdot 1 = 10$ satisfies $10^2 \equiv 2 \bmod 49$. If $c^2 \equiv 2 \bmod 49$, this says $(x/c)^2 \equiv 1 \bmod 49$, and by problem 6 , this means $x/c \equiv \pm 1 \bmod 49$ so $x \equiv \pm c \bmod 49$. This says the solutions to $x^2 \equiv 2 \bmod 49$ are $x \equiv \pm 10 \bmod 49$.

Hensel's lemma can't tell us anything about squares mod 2^k, because the derivative condition is never met. However, this case is fairly easy to deal with.

Proposition 1. *Let a be an odd integer. Then $a \equiv 1 \bmod 8$ if and only if a is a square mod 2^k for $k \geq 3$.*

Proof. Suppose that $a \equiv c_k^2 \bmod 2^k$ for $k \geq 3$. Then clearly $a \equiv c_k^2 \bmod 8$, and the only non-zero square mod 8 is 1, so $a \equiv 1 \bmod 8$. Conversely, suppose that $a \equiv 1 \bmod 8$. We'll inductively construct c_k such that $a \equiv c_k^2 \bmod 2^k$ for $k \geq 3$. By assumption, $c_3 = 1$. Now suppose that c_k exists for some $k \geq 3$. Then $a \equiv c_k^2 \bmod 2^k$ says $a = c_k^2 + 2^k\ell$ for some ℓ. Define $c_{k+1} = c_k + 2^{k-1}\ell$, and note that $c_{k+1}^2 = (c_k + 2^{k-1}\ell)^2 = c_k^2 + 2^k\ell + 2^{2k-2}\ell^2 = a + 2^{2k-2}\ell^2$. Since $k \geq 3$, we have $2k-2 \geq k+1$, so $c_{k+1}^2 \equiv a \bmod 2^{k+1}$ as desired. Therefore by induction, we have shown that a is a square mod 2^k for any $k \geq 3$. □

Combining these two results gives us a criterion for checking when an integer a is a quadratic residue mod n.

Theorem 0.4. *Let $n = 2^e p_1^{e_1} \cdots p_k^{e_k}$ be a factorization into primes with $e \geq 0$ and let a be an integer with $\gcd(a, n) = 1$.*

(i) *If $e = 0, 1$, then a is a square mod n if and only if a is a square mod p_i for all i.*
(ii) *If $e = 2$ then a is a square mod n if and only if $a \equiv 1 \bmod 4$ and a is a square mod p_i for all i.*
(iii) *If $e \geq 3$, then a is a square mod n if and only if $a \equiv 1 \bmod 8$ and a is a square mod p_i for all i.*

Proof. The proof of all three statements will be largely the same: if $a \equiv c^2 \bmod n$, then clearly $a \equiv c^2 \bmod 2^e$ and $a \equiv c^2 \bmod p_i^{e_i}$ for all i, so $a \equiv c^2 \bmod p_i$ for all i. If $e = 2$, then the only non-zero square mod 4 is 1, so $a \equiv 1 \bmod 4$. If $e \geq 3$, we have $a \equiv 1 \bmod 8$ by the above proposition. Now suppose that a is a square mod p_i for all i. By Hensel's lemma, we saw earlier that a is a square mod $p_i^{e_i}$ for all i. If $e = 1$ then $a \equiv 1 \bmod 2$. If $e = 2$, then $a \equiv 1 \bmod 4$ means that a is a square mod 4, and if $e \geq 3$ the above proposition says that $a \equiv 1 \bmod 8$ means a is a square mod 2^e. Let $f(x) = x^2 - a$. Since $f(x) \equiv 0 \bmod 2^e$ is solvable and $f(x) \equiv 0 \bmod p_i^{e_i}$ is solvable for all i, by problem 2 we have that $f(x) \equiv 0 \bmod 2^e p_1^{e_1} \cdots p_k^{e_k}$ is solvable, i.e. a is a square mod n as desired. □

The above theorem tell us the Jacobi symbol still retains some information about whether a is a square mod n or not.

Corollary 0.5. *Let n be an odd integer and a an integer with $\gcd(a,n) = 1$. Then if $\left(\frac{a}{n}\right) = -1$, then a is not a square mod n. Equivalently, if a is a square mod n, then $\left(\frac{a}{n}\right) = 1$.*

Proof. Write $n = p_1^{e_1} \cdots p_k^{e_k}$. By definition, we have $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}$. Saying $\left(\frac{a}{n}\right) = -1$ means that $\left(\frac{a}{p_i}\right) = -1$ for some i, i.e. a is not a square mod p_i for some i. By the above theorem, this means a is not a square mod n. The second statement follows by taking the contrapositive of the first. □

As an application of the above theorem, we give the following example of a so *local-global* principle.

Theorem 0.6. *Let n be an integer. Then n is a square in $\mathbb{Z}$ if and only if n is a square mod p for all primes p.*

Proof. If $n = k^2$ then clearly $n \equiv k^2 \bmod p$ for any prime p. For the more interesting direction, suppose that n is a square mod p for all prime p but n is not a square in $\mathbb{Z}$. Then we can write $n = a^2 p_1 \cdots p_k$ for some primes p_i. We will construct an integer N with $\left(\frac{n}{N}\right) = -1$, so that by the above corollary, n is not a square mod N, so that n is not a square mod some prime p dividing N. This will give us a contradiction. To do so, first note that at least one of the primes p_i must be odd. Otherwise, $n = 2a^2$, so $n \equiv 2 \bmod 3$ which contradicts that n is a square mod 3. Let $p_1, \ldots, p_\ell$ be the odd primes among $p_1, \ldots, p_k$. Consider the system of congruences

$$\begin{cases} x \equiv 1 \bmod 8 \\ x \equiv b \bmod p_1 \\ x \equiv 1 \bmod p_2 \\ \vdots \\ x \equiv 1 \bmod p_\ell \end{cases}$$

where b is any non-square mod p_1. By the Chinese remainder theorem, there is an integer N solving this system. By taking the power of 2 out of the squared part of n if necessary, write $n = 2^k a'^2 p_1 \cdots p_\ell$ for some a' and some k. Then $\left(\frac{n}{N}\right) = \left(\frac{2^k a'^2 p_1 \cdots p_\ell}{N}\right) = \left(\frac{2}{N}\right)^k \left(\frac{p_1}{N}\right) \cdots \left(\frac{p_\ell}{N}\right) = \left(\frac{N}{p_1}\right) \cdots \left(\frac{N}{p_\ell}\right) = -1$ by Jacobi reciprocity and the fact that $\left(\frac{2}{N}\right) = 1$ because $N \equiv 1 \bmod 8$. We've reached our desired contradiction, so n must be a a square in $\mathbb{Z}$ as desired. □