SOME AMAZING PROPERTIES OF THE FUNCTION $f(x) = x^2$ *

David M. Goldschmidt
University of California, Berkeley
U.S.A.

1. Introduction

Today we are going to have a look at one of the simplest functions in mathematics, $f(x) = x^2$, but from a point of view which may not be familiar to you. Namely, we are going to study the *arithmetic* properties of this function, which is just a fancy way of saying that we will restrict its arguments to be integers.

The question of which whole numbers are squares of whole numbers, and what sorts of properties they have, is an old and honorable one. Near the beginning of the nineteenth century, the famous German mathematician Gauss discovered a deep and elegant property of these integral squares, which he called the "law of quadratic reciprocity". Towards the end of the same century, another German mathematician, Hilbert, initiated a program of research which culminated in the 1920's with a far-reaching generalization of the law of quadratic reciprocity. It is safe to say that this work, which is today known as "class-field theory", will stand as one of the major achievements of twentieth century mathematics.

In this talk, I will approach quadratic reciprocity from a point of view which, although quite elementary, is in the spirit of what the generalizations are all about.

2. Quadratic Residues

One of the most interesting of the many innovations developed by Gauss is the idea of *congruences.* Namely, for integers a, b, and n, we write $a \equiv b \pmod{n}$ provided that the difference $a - b$ is evenly divisible by n. Gauss's idea was that the symbol "$\equiv$" can be thought of as a weakened version of "$=$". That is, if $a = b$ then a and b are certainly congruent since their difference, being zero, is divisible by any n. Furthermore, if we choose a fixed "modulus", n, then given $a \equiv a'$ and $b \equiv b'$ one can easily check that

$$a + b \equiv a' + b'$$
$$a - b \equiv a' - b'$$
$$ab \equiv a'b'$$

These relations enable us to perform arithmetic "modulo n" which, as we shall see, is a very powerful technique.

Now, an obvious necessary condition for an integer a to be a square is that it be congruent to a square modulo n, for any n. But for small values of n, this condition is very easily checked. For example, if the equation $x^2 = 12,345,678$ had

*Lecture delivered at the National University of Singapore on 1st September 1981.

an integer solution, the congruence $x^2 \equiv 8 \pmod{10}$ would have a solution. But since any integer x is congruent modulo 10 to an integer between 0 and 9, and since we can easily check that

$$0^2 \equiv 0 \qquad 1^2 \equiv 1 \qquad 2^2 \equiv 4 \qquad 3^2 \equiv 9$$
$$4^2 \equiv 6 \qquad 5^2 \equiv 5 \qquad 6^2 \equiv 6 \qquad 7^2 \equiv 9$$
$$8^2 \equiv 4 \qquad 9^2 \equiv 1$$

it follows that the congruence $x^2 \equiv a \pmod{10}$ has a solution if and only if a is congruent modulo 10 to one of 0, 1, 4, 5, 6, 9. In particular, 12, 345, 678 cannot be a square.

We have in the above exploited the fact that every integer a is congruent modulo n to its remainder upon division by n. That is, we can always reduce the fraction a/n to "lowest terms", obtaining

$$a/n = q + r/n$$

where q is an integer and $0 \leqslant r < n$. Then $a - r = nq$ is evenly divisible by n, so a is congruent to r modulo n. It is therefore convenient to call the set of integers $\{ a \mid 0 \leqslant a < n \}$ the set of "residues mod n" since every integer is congruent to one of these. Indeed, since the difference of any two distinct residues has absolute value less than n, no two of them are congruent to each other, so every integer is congruent to exactly one of these residues.

For n = 10, we computed above that not all ten of the residues are "quadratic". In fact, there are exactly 5 non-zero residues a for which the congruence $x^2 \equiv a \pmod{10}$ has a solution, namely $\{ 1, 4, 5, 6, 9 \}$. In general, we let Q(n) denote the set of non-zero quadratic residues mod n. That is, Q(n) is the set of all non-zero residues a for which the congruence $x^2 \equiv a \pmod{n}$ has a solution. We exclude zero since $x^2 \equiv 0$ always has a trivial solution.

Notice that to find the set Q(n), we can simply reduce to lowest terms all the fractions $\{ a^2/n \mid 0 \leqslant a < n \}$ and take all the distinct remainders. Thus, since $(n - a)^2 \equiv (-a)^2 = a^2$, we can never get more than $(n - 1)/2$ distinct quadratic residues. But sometimes we get less, for example we have

$$1^2 \equiv 4^2 \equiv 14^2 \pmod{15}$$

so there are fewer than 7 quadratic residues modulo 15 (in fact, there are only 5). When n is a prime, however, we get

Lemma 1: Let p be an odd prime. Then the cardinality of Q(p) is $(p - 1)/2$.

Proof. The congruence $a^2 \equiv b^2 \pmod{p}$ means that p divides $a^2 - b^2 = (a - b)(a + b)$. But whenever a prime divides a product, it must divide one of the factors, so we get $a \equiv \pm b \pmod{p}$. In other words, if a and b are distinct residues mod p and $a^2 \equiv b^2 \pmod{p}$ then $a = p - b$, so there are exactly $(p - 1)/2$ distinct quadratic residues mod p.

3. The Function $f_p(n)$.

As we saw in lemma 1, the quadratic residues seem to be "better behaved" when the modulus is a prime, so in this section we let p be a fixed odd prime and we obtain some further properties of the set Q(p).

Lemma 2: Let a and b be integers. Then $(a+b)^p \equiv a^p + b^p \pmod p$.

Proof. By the binomial theorem, we have

$$(*) \qquad (a+b)^p = a^p + pa^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + pab^{p-1} + b^p$$

Consider the binomial coefficient

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1} \qquad (0<k<p).$$

This is a rational fraction which is in fact an integer. Since $k<p$, p does not divide the denominator, but p does divide the numerator and therefore p divides the quotient. In particular, all terms in the right-hand-side of (*) except possibly the first and last are divisible by p, whence the lemma.

Corollary: Let n be any integer, then $n^p \equiv n \pmod p$. If $n \not\equiv 0 \pmod p$ then $n^{p-1} \equiv 1 \pmod p$.

Proof. It suffices to prove this for $n>0$ (in fact, for $0 \leqslant n < p$) so we proceed by induction, the case n = 0 being trivial. We have $(n+1)^p \equiv n^p + 1$ by lemma 2 and, assuming that $n^p \equiv n \pmod p$, the first assertion follows by induction. Now, since p divides $n^p - n = n(n^{p-1} - 1)$, p must divide one of the factors, and the remaining assertion follows.

Next, for any interger $n \not\equiv 0 \mod p$, let $\overline{n}$ be the residue of n mod p, and define

$$f_p(n) = \begin{cases} +1, \text{ if } \overline{n} \in Q(p) \\ -1, \text{ if } \overline{n} \notin Q(p) \end{cases}$$

Lemma 3. For any integer $n \not\equiv 0 \pmod p$, $f_p(n) \equiv n^{(p-1)/2} \pmod p$.

Proof. Given any polynomial

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

with integer coefficients, and any integer a, we can divide g(x) by x − a obtaining

$$g(x) = g_a(x)(x-a) + g(a)$$

where $g_a(x)$ is a polynomial of degree n − 1 with integer coefficients, and the same leading coefficient as g(x). It follows that if $g(a) \equiv 0 \pmod p$, then $g(x) \equiv g_a(x)(x-a)$, where this congruence of polynomials means that coefficients of corresponding powers of x are congruent. Now apply the above to the polynomial $g(x) = x^{(p-1)/2} - 1$, and any integer $a_1 \in Q(p)$. Since $a_1 \equiv b^2$ for some integer b, we

have $a_1^{(p-1)/2} \equiv b^{p-1} \equiv 1$ by the corollary to lemma 2. Therefore, there is a polynomial $g_1(x)$ of degree $(p-3)/2$ with integral coefficients and leading coefficient 1, such that

$$g(x) \equiv g_1(x)(x - a_1) \pmod{p}$$

Now choose $a_2 \in Q(p) - \{a_1\}$, then $g(a_2) \equiv 0$ as before, so p divides $g_1(a_2)(a_2 - a_1)$. Since $a_2 \not\equiv a_1$, we get $g_1(a_2) \equiv 0$. Thus, we can divide again, obtaining

$$g_1(x) \equiv g_2(x)(x - a_2)$$

for some polynomial $g_2(x)$ of degree $(p-5)/2$ with integral coefficients and leading coefficient 1. Putting these together we get

$$g(x) \equiv g_2(x)(x - a_1)(x - a_2).$$

Continuing in this way, we eventually obtain

$$g(x) \equiv g_{(p-1)/2}(x)(x - a_1)(x - a_2) \ldots (x - a_{(p-1)/2})$$

where $g_{(p-1)/2}(x)$ is a polynomial of degree zero with leading coefficient 1 and $Q(p) = \{a_1, a_2, \ldots, a_{(p-1)/2}\}$. In other words, we have proved that

$$(*) \qquad x^{(p-1)/2} - 1 \equiv \prod_{a \in Q(p)} (x - a) \pmod{p}.$$

We have already observed that $x^{(p-1)/2} \equiv 1$ if $\bar{x} \in Q(p)$. Now (*) shows that $x^{(p-1)/2} \not\equiv 1$ if $\bar{x} \notin Q(p)$. But the corollary to lemma 2 shows that

$$(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = x^{p-1} - 1 \equiv 0$$

for all $x \not\equiv 0 \pmod{p}$. Hence for $\bar{x} \notin Q(p)$, we must have $x^{(p-1)/2} \equiv -1 \pmod{p}$, and the lemma follows.

Corollary: $f_p(n)f_p(m) = f_p(nm)$ for all integers $n, m \not\equiv 0 \pmod{p}$.

Proof. Since $(mn)^{(p-1)/2} = m^{(p-1)/2}n^{(p-1)/2}$, lemma 3 shows that $f_p(n)f_p(m) \equiv f_p(mn) \pmod{p}$. But the congruence must be an equality since $-1 \not\equiv +1$ (p is odd!).

4. Roots of Unity

In this section, we assemble some elementary facts about the complex roots of unity which we need in order to obtain the deeper properties of the function $f_p(n)$.

Let m be an integer, and let w_m be the complex number

$$e^{2\pi i/m} = \cos(2\pi/m) + i \sin(2\pi/m)$$

One easily checks that w_m is a *primitive* m^{th} *root of unity,* that is, $w_m{}^m = 1$, while $w_m{}^i \neq 1$ for $0 < i < m$.

Now let R_m be the set of all complex numbers of the form

$$\sum_{i=0}^{m-1} a_i w_m{}^i$$

where the a_i are integers. It's easy to see that sums and integral multiples of complex numbers of this form are still of this form. In addition, if $n = qm + i$ with $0 \leq i < m$, then $w_m{}^n = w_m{}^i$ from which it follows that R_m is also closed under taking *products.* We can therefore think of R_m as a sort of generalization of the integers. In fact, it is an example of what is called a *ring of algebraic integers.*

We are going to define congruences in R_m and use them to study the function $f_p(n)$. Namely, if $x, y, z \in R_m$ we write $x \equiv y \pmod{x}$ if $x - y = uz$ for some number $u \in R_m$. It is easy to check that one can add, subtract, and multiply these congruences, just as with ordinary congruences on integers. However, in order to know that the relation of congruence is non-trivial in R_m, the following lemma is helpful.

Lemma 4: The only rational numbers in R_m are integers.

Proof. This is an exercise in linear algebra. Suppose that r is a rational rumber in R_m. Then for each $j = 1, 2, \ldots m$ there exist integers a_{ij} $(i = 1, 2, \ldots, m)$ such that

$$rw_m{}^j = \sum_{i=1}^{m} a_{ij} w_m{}^i.$$

Thus, the system of linear equations

$$\sum_{i=1}^{m} (a_{ij} - \delta_{ij} r) x_j = 0$$

(where δ_{ij} is the Kronecker symbol) has a non-zero solution over the complex numbers. Since the coefficients are rational, however, it has a non-trivial solution over the rational numbers. By clearing denominators carefully, we can find an integer solution b_j $(j = 1, 2, \ldots, m)$ whose GCD is 1. Thus there are integers c_j with

$$\sum_{j=1}^{m} b_j c_j = 1.$$

Multiplying the j^{th} equation by c_j and summing over j yields

$$\sum_{i,j} a_{ij} b_j c_j - \sum_{i,j} \delta_{ij} r b_j c_j = 0$$

$$r = \sum_{i,j} a_{ij} b_j c_j.$$

Notice that since R_m contains the integers, it makes sense to consider congruences in R_m modulo the same prime integer p as before. Thus we record

Lemma 5: If $x, y \in R_m$ then $(x + y)^p \equiv x^p + y^p \pmod{p}$.

Proof. This follows from the binomial theorem, exactly as before.

Lemma 6: $n^{1/2} \in R_{4n}$, for any integer n.

Proof. Clearly, it suffices to show that $p^{1/2} \in R_{4n}$ for all primes p which divide n. If $p = 2$, let $n = 2k$ then $w_{4n}^{\,k}$ is a primitive 8^{th} root of unity, and one checks that $w_{4n}^{\,k} + w_{4n}^{\,-k} = 2^{1/2}$. For p odd, we let $n = pk$ and let $u = w_{4n}^{\,4k}$, then u is a primitive p^{th} root of unity. Observing that $\{1, u, u^2, \ldots, u^{p-1}\}$ is the set of all roots of the polynomial $x^p - 1$, we have

$$x^p - 1 = \prod_{i=0}^{p-1} (x - u^i)$$

Dividing both sides by $x - 1$ and substituting $x = 1$ into the resulting equation yields the identity

$$(*) \qquad \prod_{i=1}^{p-1} (1 - u^i) = p.$$

Next, notice that $1 - u^i = -u^i(1 - u^{p-i})$, so that multiplying (*) by

$$(-1)^{(p-1)/2} u u^2 \ldots u^{(p-1)/2},$$

and letting

$$d = \prod_{i=1}^{(p-1)/2} (1 - u^i)$$

(*) becomes

$$(-1)^{(p-1)/2} u^{(p^2-1)/8} d^2 = p.$$

Since -1 and u are both squares in R_{4n} (this is the reason for taking $4n$ instead of n) it follows that p is a square as well.

Finally, we need to record an important fact about R_m. The proof would take us too far afield here, but can be found in any textbook on Galois Theory.

Lemma 7: For each prime p not dividing m, there exists a unique function $s_p : R_m \to R_m$ with the following properties:

(1) $s_p(w_m) = w_m{}^p$

(2) $s_p(n) = n$ for all integers n

(3) $s_p(x + y) = s_p(x) + s_p(y)$

(4) $s_p(xy) = s_p(x)\, s_p(y)$.

for all $x, y \in R_m$

5. A conductor for $f_p(n)$

We have thus far been studying the function $f_p(n)$ for fixed p and variable n. For example, the corollary to lemma 3 showed us that $f_p(n)$ is multiplicative in n, which, although interesting enough, is perhaps not all that surprising. Now, however, we are going to stand on our heads, so to speak, by fixing n and letting p vary. At first sight, this idea seems ridiculous. What possible connnection can there be between the quadratic character of a particular integer n modulo *different* primes? The amazing facts are as follows:

THEOREM: Let n be a fixed integer and let p, q and r be odd primes not dividing n.

(1) If $p \equiv q \pmod{4n}$, then $f_p(n) = f_q(n)$.

(2) If $pq \equiv r \pmod{4n}$ then $f_p(n) f_q(n) = f_r(n)$.

Let's pause a moment to consider the strength of this result. Question: Is 5 a quadratic residue modulo 101? Since $101 \equiv 3.7 \pmod{20}$, the theorem says that $f_{101}(5) = f_3(5)\, f_7(5) = (-1)(-1) = 1$. Before reading further, try to find an integer a such that $a^2 \equiv 5 \pmod{101}$.

Proof of theorem: Let $m = 4n$ and let $u \in R_m$ with $u^2 = n$ (see lemma 6). Let p be an odd prime not dividing n. Then $u^p = uu^{2(p-1)/2} = un^{(p-1)/2}$, so using lemma 3 we obtain

$$(*) \qquad u^p \equiv f_p(n)u \pmod{p}.$$

Now let s_p be the function of lemma 7, then

$$s_p(u)^2 = s_p(u^2) = s_p(n) = n.$$

On the other hand, let $x = \sum_{i=0}^{m-1} a_i w_m^{\,i}$ for any integers a_i. Then corollary to lemma 2 together with lemmas 5 and 7 can be combined to obtain

$$s_p(x) = \sum_{i=0}^{m-1} a_i w_m^{\,ip} \equiv x^p \pmod{p}.$$

In particular, $s_p(u) \equiv u_p \pmod{p}$, so (*) now gives us

$$(**) \qquad s_p(u) \equiv f_p(n)u \pmod{p}.$$

However, we have seen above that $s_p(u)^2 = n$, so we must have $s_p(u) = \pm f_p(n)u$. In the latter case, we get $-1 \equiv +1 \pmod{p}$, which leads to an equation $pz = 2$ for some $z \in R_m$. But this contradicts lemma 4, since 2/p is not an integer. So the former case must hold, i.e. we have

$$(***) \qquad s_p(u) = f_p(n)\,u.$$

Now it is easy to complete the proof. Suppose that $p \equiv q \pmod{m}$. Then $w_m^{\,p} = w_m^{\,q}$, so we have $s_p = s_q$ by lemma 7 and therefore $f_p(n) = f_q(n)$ by (***). Suppose that $pq \equiv r \pmod{m}$, then $w_m^{\,pq} = w_m^{\,r}$ so lemma 7 implies that $s_q(s_p(x)) = s_r(x)$ for all $x \in R_m$. Now apply s_q to both sides of (***) to get $f_p(n)f_q(n) = f_r(n)$.

Now that you have seen the proof, go ahead and convince yourself that it works by dividing 45^2 by 101 and finding the remainder!