Analytic number theory and quadratic reciprocity

Levent Alpoge

March 31, 2013

Abstract

What could the myriad tools of analytic number theory for proving bounds on oscillating sums possibly have to say about algebra? Quite a lot! We take the vaunted quadratic reciprocity law of Gauss and prove it by bounding exponential sums sufficiently well. In the process we introduce some of the standard techniques of analytic number theory. Secretly the point of this article is to motivate these surely analytic methods with an algebraic problem.

1 Introduction

Learning analytic number theory is difficult, in no small part because many of the methods seem totally ad hoc to the uninitiated learner. It is tremendously easier to learn the subject with a problem in mind, and surely the law of quadratic reciprocity qualifies as a nice problem. Of course, it is not at all clear how analysis might be brought to bear on quadratic residues modulo primes.

Really the point of this article is to present a bunch of beautiful things to the reader in the guise of an analytic proof of an algebraic fact. Of course there are much faster and clearer proofs of the law! But certainly there can never be enough. We press on.

Theorem 1 (Quadratic Reciprocity)**.** *Let $p \neq q$ be odd primes.*
Then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

As a reminder, by $\left(\frac{a}{p}\right)$ we mean the usual Legendre symbol: 1 if a reduces to a square modulo p, 0 if p divides a, and -1 otherwise. (So, for instance, $1+\left(\frac{a}{p}\right)$ is the number of square roots of a modulo p.) By a theorem of Euler, this is congruent to $a^{\frac{p-1}{2}}$ modulo p.

2 Gauss sums

Some notation. We write

$$e(x) := e^{2\pi i x},$$

so that the usual Fourier transform of a nice function f is

$$\hat{f}(\xi) = \int_{\mathbb{R}} f(x)e(-x\xi)dx.$$

Observe that $e(\cdot) : \mathbb{R} \to \mathbb{C}$ descends to a map out of $\mathbb{R}/\mathbb{Z}$. So, for instance, given an element $\alpha \in \mathbb{Z}/n\mathbb{Z}$, it makes sense to write $e(\alpha/n)$. Finally, we'll write $(\mathbb{Z}/n\mathbb{Z})^\times$ for the group of multiplicative units of $\mathbb{Z}/n\mathbb{Z}$.

Here is a brilliant leap forward, due to Gauss.

Definition 2. *Let p be an odd prime. The* quadratic Gauss sum *modulo p is:*

$$g(p) := \sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k^2/p).$$

We will abuse notation and generalize this definition slightly.

Definition 3. *Let n be a positive integer, and $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ a homomorphism (or "character"). The* Gauss sum *associated to χ is:*

$$G(\chi) := \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(k) e(k/n).$$

The first thing to remember is that

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$$

is a homomorphism. Whence generalization?

Proposition 4. *Let p be an odd prime.*
Then:

$$G\left(\left(\frac{\cdot}{p}\right)\right) = g(p).$$

Proof. Let's write out the left-hand side.

$$\begin{aligned} G\left(\left(\frac{\cdot}{p}\right)\right) &= \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(k) e(k/p) \\ &= \sum_{0 \neq k = \square} e(k/p) - \sum_{k \neq \square} e(k/p), \end{aligned}$$

where all sums are over $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ and our joking notation $k = \square$ has the (hopefully) obvious meaning (that k is a square).

Now, note that

$$\sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k/p) = 0.$$

(Multiply the left-hand side by $e(1/p) \neq 1$ for an easy proof.) So that sum over nonsquares, which — remember! — did *not* include zero, is therefore:

$$\sum_{0 \neq k \neq \square} e(k/p) = -1 - \sum_{k = \square} e(k/p).$$

The only thing left to note is that, in $(\mathbb{Z}/p\mathbb{Z})^\times$, every nonzero square has exactly two square roots, while $0 \in \mathbb{Z}/p\mathbb{Z}$ has exactly one. $\square$

Remark 5. The Gauss sums have brothers: Jacobi sums. The two together are analogues of the Gamma and Beta functions of analysis. Using these Jacobi sums, one can, for instance, show that 2 is a cube modulo an odd prime $p \equiv 1 \pmod 3$ if and only if $p = A^2 + 27B^2$ has a solution over $\mathbb{Z}$. Go read Ireland and Rosen for more! (I think this observation was first due to Elkies.) These are the usual Gauss sums that come up everywhere in number theory, but we won't see them again — it will be enough to deal with the $g(p)$.

Great, so I've told you a totally ad hoc definition after waxing poetic about how hard it is to learn from such stuff. But at least we see the Legendre symbol in there — so that's a start.

Here is another generalization that might have been tugging at you.

Definition 6. *Let n be a positive integer. The* quadratic Gauss sum *modulo n is:*

$$g(n) := \sum_{k \in \mathbb{Z}/n\mathbb{Z}} e(k^2/n).$$

Now, writing down the very first definition probably does take a Gauss, because the following miracle relates it to our question.

Proposition 7. *Let $p \neq q$ be odd primes.*
Then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{g(p)g(q)}{g(pq)}.$$

(We'll see in a moment that $g(pq) \neq 0$ and so such a division actually makes sense.)

Proof. There's really only one thing to do: look at $g(p)g(q)$ and hope for the best. So we do that. We get:

$$g(p)g(q) = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{a^2q + b^2p}{pq}\right).$$

Now remember the Chinese remainder theorem:

$$\mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

via

$$\alpha \mapsto (\alpha \bmod p, \alpha \bmod q)$$

is an isomorphism. But under this map

$$a^2q + b^2p \mapsto \left(a^2q, b^2p\right).$$

But the squares of $\mathbb{Z}/pq\mathbb{Z}$ are precisely those that reduce to squares in each slot:

$$\square = (\square, \square).$$

So maybe we should have been more clever to start.

Since p and q are relatively prime, we can find integers P and Q for which:

$$pQ + Pq = 1.$$

Note that, then,

$$pQ \equiv 1 \pmod{q},$$

and

$$Pq \equiv 1 \pmod{p}.$$

Let's take such P, Q. Note that

$$\sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k^2/p) = \left(\frac{q}{p}\right) \sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k^2 P/p),$$

just because

$$\sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k/p) = 0,$$

as noted before (remember the minus sign!). Hence we might have started with:

$$g(p)g(q) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{a^2 Pq + b^2 pQ}{pq}\right).$$

But now we are in good shape. The reduction map takes

$$a^2 Pq + b^2 pQ \mapsto \left(a^2, b^2\right) = (a, b)^2,$$

and so as a and b run over $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, respectively, $a^2 Pq + b^2 pQ$ runs over the squares of $\mathbb{Z}/pq\mathbb{Z}$ taken with the appropriate multiplicities. That is to say, this last expression is exactly

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \sum_{\alpha \in \mathbb{Z}/pq\mathbb{Z}} e(\alpha^2/pq) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) g(pq),$$

as desired. □

OK, now for a big theorem.

Theorem 8. *Let n be an odd integer.*
Then:

$$|g(n)| = \sqrt{n}.$$

In particular, $g(p) \neq 0$ always, and so $g(p)g(q) \neq 0$ for $p \neq q$ odd primes. So indeed the division above was not suspect, since we showed that $0 \neq g(p)g(q) = \pm g(pq)$ above.

Proof. We just follow our noses and calculate what we can.

So we'll instead figure out

$$\begin{aligned} |g(n)|^2 &= g(n)\overline{g(n)} \\ &= \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \sum_{\ell \in \mathbb{Z}/n\mathbb{Z}} e\left(\frac{k^2 - \ell^2}{n}\right) \\ &= \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \sum_{\ell \in \mathbb{Z}/n\mathbb{Z}} e\left(\frac{(k-\ell)(k+\ell)}{n}\right). \end{aligned}$$

Via $(k, \ell) \mapsto (k + \ell, k - \ell)$, this becomes

$$\sum_{k \in \mathbb{Z}/n\mathbb{Z}} \sum_{\ell \in \mathbb{Z}/n\mathbb{Z}} e\left(\frac{4k\ell}{n}\right).$$

The fact that n is odd tells us that that factor of 4 can be absorbed into e.g. ℓ. In any case, the inner sum is zero for $k \not\equiv 0 \bmod n$ (again, multiply by $e(k/n) \neq 1$). Otherwise it is, of course, n. (Interjection: $k = 0$ now corresponds to $k = \ell$ in the earlier variables. Thus it stands to reason that this is called the "diagonal contribution", which is evidently dominant. This sort of dichotomy occurs all over the place.) That is to say, our calculation reveals:

$$|g(n)|^2 = n,$$

as desired.

□

Let's slow down for a second and take stock of what we've just proved. We have some strange sum of $\asymp q$ phases on the unit circle and it ends up being of absolute value $\sqrt{q}$. But actually the phases are really complicated: they secretly depend on some mysterious χ (the Legendre symbol) and also keep twisting around according to this exponential. What a random combination! Well, random is a funny word: let's actually act like we'd been choosing (uniformly) *random* phases off the unit circle and summing up q of them. Well, if q is large, this should (sort of) ring a bell. That is, we're summing a bunch of independent and identically distributed random variables (with, say, finite variance), and the *central limit theorem* (pardon the bell pun earlier…) tells us to expect the thing to be precisely on the order of $\sqrt{n}$. So we could have guessed the answer by giving up on the algebraic structure in advance!

So it stands to reason that the absolute value of $g(p)$ can't possibly tell us anything deep like quadratic reciprocity. And there is only one thing left: the phase. So this big theorem has been reduced to calculating the phase of some exponential sums.[1]

3 The sign of the Gauss sum

Why "sign" and not "phase"?

Proposition 9. *Let n be a positive integer and $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{R}^\times = \{\pm 1\}$ a homomorphism. Then:*

$$\overline{G(\chi)} = \chi(-1)G(\chi).$$

Proof.

$$\overline{G(\chi)} = \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(n)e(-k/n).$$

Now change variables via $k \mapsto -k$. □

[1] Now we can see analysis creeping in: $-n$ is very far from n! That was essentially my line of thinking when coming up with this…

So we find that:

Corollary 10. *Let $p \neq q$ be odd primes.*
Then:

$$g(p) = \begin{cases} \pm\sqrt{p} & p \equiv 1 \bmod 4, \\ \pm i\sqrt{p} & p \equiv 3 \bmod 4, \end{cases}$$

and

$$g(pq) = \begin{cases} \pm\sqrt{pq} & pq \equiv 1 \bmod 4, \\ \pm i\sqrt{pq} & pq \equiv 3 \bmod 4. \end{cases}$$

Let's write $\epsilon(n)$ for the sign of the Gauss sum: that is, so that

$$g(p) = \epsilon(p)\sqrt{p} \begin{cases} 1 & p \equiv 1 \bmod 4, \\ i & p \equiv 3 \bmod 4 \end{cases}.$$

So we're almost there. Gauss also got to this point pretty easily and wanted to know the sign as well (likely for the exact same reason: quadratic reciprocity). So he did a bunch of examples and came up with a conjecture. Go ask your computer for $\epsilon(p)$ for $p = 3, 5, 7, 11, 13, \ldots$. I did, and here's what I got:

$$\begin{aligned} \epsilon(3) &= +1, \\ \epsilon(5) &= +1, \\ \epsilon(7) &= +1, \\ \epsilon(11) &= +1 \\ \epsilon(13) &= +1. \end{aligned}$$

See a pattern? How about $\epsilon(pq)$? Well,

$$\epsilon(15) = +1, \epsilon(21) = +1,$$

and

$$\epsilon(33) = +1.$$

So maybe:

Conjecture 11. *Let $p \neq q$ be odd primes.*
Then:

$$\epsilon(p) = \epsilon(pq) = +1.$$

What does this have to do with quadratic reciprocity? Everything! Assume the above conjecture.

Proof of Theorem 1 assuming Conjecture 11. By Proposition 7,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{\left(\begin{cases} 1 & p \equiv 1 \bmod 4, \\ i & p \equiv 3 \bmod 4. \end{cases}\right)\left(\begin{cases} 1 & q \equiv 1 \bmod 4, \\ i & q \equiv 3 \bmod 4. \end{cases}\right)}{\left(\begin{cases} 1 & pq \equiv 1 \bmod 4, \\ i & pq \equiv 3 \bmod 4. \end{cases}\right)}.$$

As strange as this may seem, that's it. □

So we "just" have to prove the conjecture. I should note here that it took Gauss *several years* to do it. So it is no joke.

4 Poisson summation and smoothing sums

Thankfully, we have Fourier analysis nowadays (actually, so did Gauss!). More precisely, we have the Poisson summation formula, which is probably one of the most important formulas in mathematics. It states:

Proposition 12. *Let $f : \mathbb{R} \to \mathbb{R}$ be a function of the Schwartz class*[2]*. Then:*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

This is, for instance, the key in proving the analytic continuation of the Riemann ζ function (and actually all Dirichlet L-functions, Hecke L-functions, ...). Its analogue over $\mathbb{F}_q$ is the Riemann-Roch formula. One can even compute the special values $\zeta(2k)$ with it! (And much more, of course.) So it is no surprise that it is the crux of the calculation.

But how can we possibly apply it? Namely, we have on our hands

$$g(n) = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} e(k^2/n),$$

a *finite* sum! Well, we're not in such bad shape. The first step in realizing this as a sum over integers is choosing representatives for the elements of $\mathbb{Z}/n\mathbb{Z}$ inside $\mathbb{Z}$ — we had might as well take them to lie in an interval. So choose some $\alpha \notin \mathbb{Z}$ (you'll see why we write the inequalities this way in a bit), and note that the set of integers k satisfying $\alpha < k < \alpha + n$ is a complete set of representatives for $\mathbb{Z}/n\mathbb{Z}$. Then

$$g(n) = \sum_{\alpha<k<\alpha+n} e(k^2/n)$$

is still a sum over integers, just not all of them. Thinking about it a little, we can of course extend this to a sum over all the integers: just write $\chi_{[\alpha,\alpha+n]}$ for the characteristic function of the interval $[\alpha, \alpha + n]$, and observe that:

$$g(n) = \sum_{k\in\mathbb{Z}} \chi_{[\alpha,\alpha+n]}(k) e(k^2/n).$$

But now the summand isn't Schwartz — it isn't even differentiable! But that's no problem.

Let $p \in C_c^\infty((\alpha, \alpha + n))$ be compactly supported in the given interval and such that $0 \leq p \leq 1, p|_{[\lceil\alpha\rceil,\lfloor\alpha\rfloor+n]} = 1$. Then p, extended by 0 to have domain all of $\mathbb{R}$, is a Schwartz function, and we still have:

$$g(n) = \sum_{k\in\mathbb{Z}} p(k) e(k^2/n).$$

We haven't changed anything except for the way we've written our sum: this is called *smoothing a sum out*. (That such a p exists is an absolutely fundamental fact in mathematics, particularly in geometry and analysis.)

[2]That is to say, f is infinitely differentiable, and for every $a, b \in \mathbb{N}$, $x^a f^{(b)}(x) \to 0$ as $|x| \to \infty$. Actually, much less stringent conditions are required of f, but we'll get away with this statement.

Now we can apply Poisson summation, and so we do:

$$g(n) = \sum_{k\in\mathbb{Z}} \int_{\alpha}^{\alpha+n} p(t) e\left(\frac{t^2}{n} - kt\right) dt.$$

5 The stationary phase method

The integrals we now have to deal with are of the shape

$$\int_{\mathbb{R}} f(x) e(\phi(x)) dx,$$

with f compactly supported. Intuitively, if ϕ is "moving quickly" — i.e., ϕ' is bounded away from zero — the factor $e(\phi(x))$ is flying randomly around the unit circle. It is moving so fast that by moving x just a little we can flip its sign. But then the contribution of the first point, say $f(x)$, is subtracted from $f(x+\epsilon)$ for ϵ very small. So now if f varies slowly, we get a bunch of terms like $f(x+\epsilon) - f(x) \approx 0$, so this integral should be *tiny*. This is made precise by integrating by parts: when $\phi'(x) \neq 0$ always,

$$\begin{aligned}\int_{\mathbb{R}} f(x) e(\phi(x)) dx &= \frac{1}{2\pi i} \int_{\mathbb{R}} \left(\frac{f(x)}{\phi'(x)}\right) \left(2\pi i \phi'(x) e^{2\pi i \phi(x)}\right) dx \\ &= -\frac{1}{2\pi i} \int_{\mathbb{R}} \left(\frac{f(x)}{\phi'(x)}\right)' e(\phi(x)) dx.\end{aligned}$$

Repeating this does even better. But it's hard to can methods in analysis, so this is as precise as I can get.

Suppose now that $\phi' = 0$ somewhere, say at X. A Taylor series expansion of ϕ would then start with

$$\phi(x) = \phi(X) + \frac{\phi''(X)}{2}(x-X)^2 + \cdots.$$

Oftentimes we are lucky enough to also have $\phi''(X) \neq 0$ (let's assume that $\phi''(X) > 0$, otherwise complex conjugate everything), so that ϕ infinitesimally looks like a quadratic plus higher-order terms about X (its critical point is called *nondegenerate*). In our case, we are so lucky. Since the higher-order terms are moving quite a bit slower, and we are assuming f to be slowly-varying, we can kill off the parts of the integral even just a little bit away from X. *Very* close to X, we may replace f by $f(X)$ and ϕ by $\phi(X) + \frac{\phi''(X)}{2}(x-X)^2$. So our integral is basically equal to

$$f(X) e(\phi(X)) \int_{|x-X|<O(1)} e\left(\frac{\phi''(X)}{2}(x-X)^2\right) dx.$$

Changing variables, this becomes:

$$f(X) e(\phi(X)) \sqrt{\frac{2}{\phi''(X)}} \int_{-O(1)}^{O(1)} e(x^2) dx.$$

Actually by the same integration by parts argument the bounds of the integral don't really matter, and this is essentially

$$f(X) e(\phi(X)) \sqrt{\frac{2}{\phi''(X)}} \int_{\mathbb{R}} e(x^2) dx.$$

This integral, the "rotated" version of the Gaussian integral, is called the *Fresnel integral*. One can calculate it by e.g. deforming it slightly to

$$\int_{\mathbb{R}} e^{2\pi i(1+i\epsilon)x^2} dx$$

and then observing that this is the Fourier transform of a nice function evaluated at zero (whence one may apply analytic continuations of standard Fourier transform identities plus the self-duality of the Gaussian — this amounts to a change of variable and a contour shift). Anyway, the end result is that[3]:

Proposition 13 (Fresnel)**.**

$$\int_{\mathbb{R}} e(x^2) dx = \frac{1+i}{2}.$$

Hence, in the end, we see that, so long as $\phi'' > 0$ where $\phi' = 0$,

$$\int_{\mathbb{R}} f(x)e(\phi(x))dx = \zeta_8 \sum_{\phi'(X)=0} \frac{f(X)e(\phi(X))}{\sqrt{\phi''(X)}} + \cdots, \tag{1}$$

where $\zeta_8 := \frac{1+i}{\sqrt{2}} = e\left(\frac{1}{8}\right)$ is a primitive eighth root of unity.

So back to our sum (with which we have to use rigor!). The k-th summand is:

$$\int_{\alpha}^{\alpha+n} p(t)e\left(\frac{t^2}{n} - kt\right) dt.$$

Applying what we've just learned, we study the zeroes of

$$\frac{2t}{n} - k$$

— i.e., we wonder if

$$\alpha \leq \frac{n}{2}k \leq \alpha + n.$$

Of course this only happens for

$$\frac{2\alpha}{n} \leq k \leq \frac{2\alpha}{n} + 2,$$

so we are in pretty good shape: *at most three* of the integrals will be negligible! Since we are lazy, let's choose

$$\alpha := -\frac{n}{4}$$

(for us n will always be odd) to make the inequalities read

$$-\frac{1}{2} \leq k \leq \frac{3}{2},$$

leaving just $k = 0$ and $k = 1$. So we expect

$$g(n) = \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t)e\left(\frac{t^2}{n}\right) dt + \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t)e\left(\frac{t^2}{n} - t\right) dt + \cdots.$$

[3]Something else that suggested that this method would work: the reader will notice that there are no minus signs: *the real and imaginary parts of the numerator are* $+1$.

But now, if we believe (1), the first integral becomes

$$\frac{1+i}{2}\sqrt{n},$$

and the second becomes

$$\frac{1+i}{2}\sqrt{n}\cdot e(-n/4).$$

That is to say,

$$g(n) = \left(\frac{1+i}{2}\right)(1+e(-n/4))\sqrt{n} + \cdots .$$

This is *exactly* what we hoped for: for $n \equiv 1 \bmod 4, (1+i)(1-i) = 2$. For $n \equiv 3 \bmod 4, (1+i)(1+i) = 2i$. I still can't get over the fact that this works.

6 A "tensor power trick" and Hensel's lemma

But of course we still have to actually make the thing mathematically rigorous[4]. Remember we imagined n was large so we could write "$\cdots$". But n *isn't* large! It could be as small as 2!

Oftentimes in mathematics one can basically prove a bound, up to let's say a constant:

$$|f(x)| \leq c|g(x)|.$$

If one can deform f and g into a *family* and prove the bound for all f and g in such a family (*with the same constant!*), then, if f^n and g^n lie in this family, we have that

$$|f(x)|^n \leq c|g(x)|^n.$$

Taking n-th powers and taking $n \to \infty$ removes the constant.

Here we have a situation where we can almost prove the result, except there may be "lower-order terms", and so we'd like to take a limit as $n \to \infty$ (and take advantage of the fact that we know that $|g(n)| = \sqrt{n}$ *exactly*). After some thought the natural thing is to replace n by n^k and take $k \to \infty$. Why? Let's focus on the case of $n = p$ an odd prime for the moment.

The claim is that the sum

$$g(p^a) = \sum_{k \in \mathbb{Z}/p^a\mathbb{Z}} e(k^2/p^a)$$

is somewhat related to

$$g(p) = \sum_{k \in \mathbb{Z}/p\mathbb{Z}} e(k^2/p).$$

But we already know the absolute values of both: $p^{\frac{a}{2}}$ and $p^{\frac{1}{2}}$, respectively. So let's try out what happens when a is odd — the best case scenario is that:

Proposition 14.

$$g(p^{2a+1}) = p^a g(p).$$

[4]Even though calculations that would qualify as heuristic don't prove anything, they are tremendously important in actually doing mathematics. So practice them!

But what are the squares modulo p^e? That is to say, given a $k \in \mathbb{Z}/p^e\mathbb{Z}$, how can we tell if the equation $t^2 - k = 0$ has a solution? Certainly by reducing further via $\mathbb{Z}/p^e\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ a solution modulo p^e will lead to one modulo p. But a lemma of Hensel tells us that that's all: once we have a solution modulo p, we can "lift" it to a solution modulo p^e for any e. (To prove the thing (and understand the extra condition), remember Newton's method of finding roots of equations!)

Lemma 15 (Hensel)**.** *Let $P \in (\mathbb{Z}/p^e\mathbb{Z})[t]$ be a polynomial such that $\bar{P} \in (\mathbb{Z}/p\mathbb{Z})[t]$, the polynomial with reduced coefficients, has a root $\xi \in \mathbb{Z}/p\mathbb{Z}$. Suppose*

$$\bar{P}'(\xi) \neq 0.$$

Then: there is a unique $\Xi \in \mathbb{Z}/p^e\mathbb{Z}$ such that

$$\overline{\Xi} = \xi$$

and

$$P(\Xi) = 0.$$

In our case, we have the polynomial $P(t) = t^2 - k$. Its reduction is $\bar{P}(t) = t^2 - \bar{k}$, with (formal) derivative

$$\bar{P}'(t) = 2t.$$

So once $\bar{k} \neq 0$, we're in good shape. Another way of saying this is that the set of squares modulo p^e certainly maps to the set of squares modulo p under the reduction map. Hensel's lemma tells us that this map is *surjective*. That is to say, the squares modulo p^e are of the form $p^{2a}b$, for $\bar{b} \neq 0$ and a square modulo p.

Proof of Proposition 14. OK. So now that we know the squares modulo p^{2a+1}, we can just calculate. Namely, in general

$$g(n) = \sum_{k=\square} \#\left|\{a \in \mathbb{Z}/n\mathbb{Z} \,|\, a^2 = k\}\right| e(k/n),$$

and so (writing the nonzero squares of $\mathbb{Z}/p^{2a+1}\mathbb{Z}$ as $p^{2e}(k + \ell p)$ with k a square modulo p and ℓ free)

$$\begin{aligned} g(p^{2a+1}) &= \#\left|\{\alpha \in \mathbb{Z}/p^{2a+1}\mathbb{Z} \,|\, \alpha^2 = 0\}\right| \\ &\quad + \sum_{e=0}^{a} \sum_{\substack{0<k<p, \\ k \equiv \square \bmod p}} \sum_{\ell \in \mathbb{Z}/p^{2(a-e)}\mathbb{Z}} \#\left|\{\alpha \in \mathbb{Z}/p^{2a+1}\mathbb{Z} \,|\, \alpha^2 = p^{2e}(k+\ell p)\}\right| e\left(\frac{p^{2e}(k+\ell p)}{p^{2a+1}}\right) \\ &= \#\left|\{\alpha \in \mathbb{Z}/p^{2a+1}\mathbb{Z} \,|\, \alpha^2 = 0\}\right| \\ &\quad + \sum_{e=0}^{a} \sum_{\substack{0<k<p, \\ k \equiv \square \bmod p}} e\left(\frac{k}{p^{2(a-e)+1}}\right) \sum_{\ell \in \mathbb{Z}/p^{2(a-e)}\mathbb{Z}} \#\left|\{\alpha \in \mathbb{Z}/p^{2a+1}\mathbb{Z} \,|\, \alpha^2 = p^{2e}(k+\ell p)\}\right| e\left(\frac{\ell}{p^{2(a-e)}}\right). \end{aligned}$$

But if $\alpha^2 = p^{2e}(k + \ell p)$, then α must be of the form $p^e\beta$ for some $\beta \in \mathbb{Z}/p^{2a+1-e}\mathbb{Z}$, with $\bar{\beta} \neq 0 \bmod p$. And indeed we are free to choose β so long as it lies over a square root of $k + \ell p$ modulo $p^{2(a-e)+1}$. But, since p is an odd prime, there are at most two square roots to choose from (even modulo a power of p) of a square: once we've found one, we write

down its negative, and that's it. That is to say, there are (at most) two choices of square root modulo $p^{2(a-e)+1}$, and then p^e times as many choices of lifts modulo p^{2a+1-e}. So the count of square roots is

$$p^e \# \left|\{\alpha \in \mathbb{Z}/p\mathbb{Z} \,|\, \alpha^2 = k\}\right|$$

for each!

Counting the number of square roots of zero is even easier: $(p^r s)^2 \equiv 0$ for $\bar{s} \neq 0$ if and only if $2r \geq 2a+1$ — i.e., the square roots of zero are precisely $p^{a+1}s$ with $s \in \mathbb{Z}/p^a\mathbb{Z}$ free to roam. That is, there are p^a many square roots of zero.

So we get:

$$g(p^{2a+1}) = p^a + \sum_{e=0}^{a} p^e \sum_{\substack{0<k<p,\\ k \equiv \square \bmod p}} \# \left|\{\alpha \in \mathbb{Z}/p\mathbb{Z} \,|\, \alpha^2 = k\}\right| e\left(\frac{k}{p^{2(a-e)+1}}\right) \sum_{\ell \in \mathbb{Z}/p^{2(a-e)}\mathbb{Z}} e\left(\frac{\ell}{p^{2(a-e)}}\right).$$

But now that inner sum is zero unless $e = a$! (— in which case there was no ℓ sum to start with!) That is,

$$\begin{aligned} g(p^{2a+1}) &= p^a \left(1 + \sum_{0 \neq k = \square \bmod p} \# \left|\{\alpha \in \mathbb{Z}/p\mathbb{Z} \,|\, \alpha^2 = k\}\right| e(k/p)\right) \\ &= p^a g(p), \end{aligned}$$

as desired. □

In fact we have the same deal for $g((pq)^{2a+1})$:

Exercise 16. *Show, using the same methods as above (and the Chinese remainder theorem), that:*

$$g((pq)^{2a+1}) = (pq)^a g(pq).$$

7 Proof

So now we can finally make everything rigorous.

Proof of Conjecture 11 (and hence Theorem 1). As before, by Poisson summation, we have that:

$$g(n) = \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t) e(t^2/n) dt + \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t) e\left(\frac{t^2}{n} - t\right) + \sum_{k \neq 0,1} \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t) e\left(\frac{t^2}{n} - kt\right) dt.$$

Replacing p by 1 in the first two integrals changes things by at most a constant. That is,

$$g(n) = \int_{-\frac{n}{4}}^{\frac{3n}{4}} e(t^2/n) dt + \int_{-\frac{n}{4}}^{\frac{3n}{4}} e\left(\frac{t^2}{n} - t\right) + \sum_{k \neq 0,1} \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t) e\left(\frac{t^2}{n} - kt\right) dt + O(1).$$

Via $t \mapsto \sqrt{n}t$ in the first integral, $t \mapsto \sqrt{n}t$ and then $t \mapsto \frac{\sqrt{n}}{2} - t$ in the second (so that the remaining integrals become the same), we get:

$$g(n) = (1 + e(-n/4)) \sqrt{n} \int_{-\frac{\sqrt{n}}{4}}^{\frac{3\sqrt{n}}{4}} e(t^2) dt + \sum_{k \neq 0,1} \int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t) e\left(\frac{t^2}{n} - kt\right) dt + O(1).$$

But

$$\begin{aligned}\int_{-\frac{\sqrt{n}}{4}}^{\frac{3\sqrt{n}}{4}} e(t^2)dt &= \int_{\mathbb{R}} e(t^2)dt + o(1)\\ &= \frac{1+i}{2} + o(1).\end{aligned}$$

That is to say,

$$g(n) = \frac{(1+i)(1+i^{-n})}{2}\sqrt{n} + o(\sqrt{n}) + \sum_{k\neq 0,1}\int_{-\frac{n}{4}}^{\frac{3n}{4}} p(t)e\left(\frac{t^2}{n} - kt\right)dt.$$

Via $t \mapsto nt$ in each of the remaining integrals,

$$g(n) = \frac{(1+i)(1+i^{-n})}{2}\sqrt{n} + o(\sqrt{n}) + n\sum_{k\neq 0,1}\int_{-\frac{1}{4}}^{\frac{3}{4}} p(nt)e\big(n(t^2-kt)\big)\,dt.$$

But now integrate by parts twice in each integral that remains (we can do this thanks to the fact that $2t-k \neq 0$ always!). The boundary terms vanish thanks to the support conditions on p. We get:

$$g(n) = \frac{(1+i)(1+i^{-n})}{2}\sqrt{n} + o(\sqrt{n}) + \frac{n}{(2\pi i)^2}\sum_{k\neq 0,1}\int_{-\frac{1}{4}}^{\frac{3}{4}}\left(\frac{\left(\frac{p(nt)}{n(2t-k)}\right)'}{n(2t-k)}\right)' e\big(n(t^2-kt)\big)\,dt.$$

But

$$\left(\frac{\left(\frac{p(nt)}{n(2t-k)}\right)'}{n(2t-k)}\right)'$$

will have four terms: in the worst case, we differentiate $p(nt)$ twice, getting $n^2p''(nt)$, and have a denominator of $n^2(2t-k)^2$. But even still, $p''(nt) = 0$ inside

$$\left[-\frac{1}{4} + \frac{\{-\frac{n}{4}\}}{n}, \frac{3}{4} - \frac{\{\frac{3n}{4}\}}{n}\right] \subseteq \left(-\frac{n}{4}, \frac{3n}{4}\right),$$

leaving an interval of length $O\big(\frac{1}{n}\big)$. Since the integrand is of absolute value at most a constant (depending on p) times $\frac{1}{(2t-k)^2} \leq O\big(\frac{1}{k^2}\big)$ anyway, the end result is that:

$$\int_{-\frac{1}{4}}^{\frac{3}{4}}\left(\frac{\left(\frac{p(nt)}{n(2t-k)}\right)'}{n(2t-k)}\right)' e\big(n(t^2-kt)\big)\,dt \leq O\left(\frac{1}{nk^2}\right),$$

and so

$$\begin{aligned}g(n) &= \frac{(1+i)(1+i^{-n})}{2}\sqrt{n} + o(\sqrt{n}) + O(1)\\ &= \frac{(1+i)(1+i^{-n})}{2}\sqrt{n} + o(\sqrt{n}).\end{aligned}$$

That is to say,

$$\frac{g(n)}{\sqrt{n}} = \frac{(1+i)(1+i^{-n})}{2} + o(1).$$

Now take $n = p^{2a+1}$ and then $n = (pq)^{2a+1}$ and take $a \to \infty$. □

References

[1] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, GTM 84, Springer-Verlag, Berlin-Heidelberg-New York, 1990.