A PRELUDE TO THE STUDY OF RECIPROCITY LAWS

JONAH SINICK

1. A case of quadratic reciprocity

Consider the set of integers that are 5 less than a square number, that is, numbers of the form $P(n) = n^2 - 5$ for $n = 1, 2, 3, \ldots$. One can ask whether there is a simple characterization of the prime factors of these numbers. Below, I've tabulated prime factorizations of these numbers for $1 \leq n \leq 45$, which I found using Magma's online calculator:

n	$P(n)$	Factorization
1	-4	-2^2
2	-1	-1
3	4	2^2
4	11	11
5	20	$2^2 \cdot 5$
6	31	31
7	44	$2^2 \cdot 11$
8	59	59
9	76	$2^2 \cdot 19$
10	95	$5 \cdot 19$
11	116	$2^2 \cdot 29$
12	139	139
13	164	$2^2 \cdot 41$
14	191	191
15	220	$2^2 \cdot 5 \cdot 11$

n	$P(n)$	Factorization
16	251	251
17	284	$2^2 \cdot 71$
18	319	$11 \cdot 29$
19	356	$2^2 \cdot 89$
20	395	$5 \cdot 79$
21	436	$2^2 \cdot 109$
22	479	479
23	524	$2^2 \cdot 131$
24	571	571
25	620	$2^2 \cdot 5 \cdot 31$
26	671	$11 \cdot 61$
27	724	$2^2 \cdot 181$
28	779	$19 \cdot 41$
29	836	$2^2 \cdot 11 \cdot 19$
30	895	$5 \cdot 179$

n	$P(n)$	Factorization
31	956	$2^2 \cdot 239$
32	1019	1019
33	1084	$2^2 \cdot 271$
34	1151	1151
35	1220	$2^2 \cdot 5 \cdot 61$
36	1291	1291
37	1364	$2^2 \cdot 11 \cdot 31$
38	1439	1439
39	1516	$2^2 \cdot 379$
40	1595	$5 \cdot 11 \cdot 29$
41	1676	$2^2 \cdot 461$
42	1759	1759
43	1844	$2^2 \cdot 461$
44	1931	1931
45	2020	$2^2 \cdot 5 \cdot 101$

A striking feature of the data is that with the exceptions of 2 and 5, *all prime numbers that appear as factors have final digit* 1 *or* 9.

For another perspective on the situation, we write out the first twenty primes, emboldening those that appear above: **2**, 3, **5**, 7, **11**, 13, 17, **19**, 23, **29**, **31**, 37, **41**, 43, 47, 53, **59**, **61**, 67, **71**. Putting aside 2 and 5, every prime number ends in 1, 3, 7 or 9. From the data, we see that of the first twenty prime numbers, all of those that end in 1 or 9 appear as prime factors of numbers of the form $n^2 - 5$, and none of those that end in 3 or 7 appear as prime factors of numbers of this form. One can verify that

the pattern persists until one is satisfied.

Conjecture 1: The prime factors of integers of the form $n^2 - 5$ are precisely 2, 5 and those primes with final digit 1 or 9.

It is remarkable that the prime factors obey such an elegant characterization. The phenomenon exhibited above is a special case of Carl Friedrich Gauss's celebrated *law of quadratic reciprocity*. In his famous 1798 book *Disquisitiones Arithmeticae*, Gauss wrote:

> *The fundamental theorem must certainly be regarded as one of the most elegant of its type.* – (Art. 151)

The general statement of quadratic reciprocity concerns prime factors of numbers of the form $P(n) = n^2 - c$ for an arbitrary, fixed, non-square c. For any such c, the law takes a form very similar to that in the case of $c = 5$. We chose to present the case that we did because in that case the pattern is visible to the naked eye as a consequence of our use of the base 10 system.

The criterion for a prime q to be a prime factor of a number of the form

$$P(n) = n^2 - c$$

is given in terms of the final digit of q in base $4c$. It is sometimes possible for the criterion to be described in terms of the final digit of q in base $2c$, or in base c. We saw above that when $c = 5$, the criterion can be described in terms of the final digit in base $2c = 10$.

In André Weil's 1940 letter to his sister Weil wrote:[1]

> *It is is beautiful and surprising that the prime numbers p for which 'a' is a residue are precisely ... those which belong to certain arithmetic progressions ... which is even more amazing, if one recalls on the other hand, that the distribution of prime numbers in any given arithmetic progression does not follow any other known law other than a statistical law ... and appears, for each concrete case that one examines numerically, to be as random as a list of numbers generated by a roulette wheel.*

We can recast Conjecture 1 into a more natural form via the following sequence of steps:

- A number has final digit 1 or 9 if and only if its remainder upon division by 10 is 1 or 9.

[1]Quotation lightly edited for context.

- Since prime numbers never have final digit 6, a prime number has remainder 1 upon division by 10 if and only if it has a remainder of 1 upon division by 5.

- Since prime numbers never have final digit 4, a prime number has remainder 9 upon division by 10 if and only if it has remainder of 4 upon division by 5.

Thus, Conjecture 1 is equivalent to:

Conjecture 1′: The prime factors of integers of the form $P(n) = n^2 - 5$ are precisely 2, 5 and those primes that leave remainder 1 or 4 upon division by 5.

2. A case of cyclotomic reciprocity

Quadratic reciprocity is very difficult to tackle head on. There is a simpler reciprocity law, called *cyclotomic reciprocity*, which is easier to establish, and which ultimately facilitates the proof of quadratic reciprocity.

There are two forms of cyclotomic reciprocity: a weak form, and a strong form. It is the strong form that facilitates the proof of the entirety of quadratic reciprocity, but the weak form is easier to state. In this set of notes, we restrict our discussion to weak cyclotomic reciprocity, treating the strong form in future set of notes.

For concreteness, in this section, we will state a special case of weak cyclotomic reciprocity, leaving the general statement to Section 8.

One simple family of polynomials with integer coefficients is the family of polynomials of the form $P(x) = x^2 - c$. The polynomials in this family are simple in the sense that they have small and fixed *degree*, but they have complexity coming from the *coefficient* c.

Another simple family of polynomials is the family of *cyclotomic polynomials*, which are obtained by varying the *degree* of the polynomial, while keeping the *coefficients* simple. This family of polynomials turns out to be easier to deal with than the quadratic polynomials from the standpoint of reciprocity laws.

The family of cyclotomic polynomials is defined to be the set of polynomials with integer coefficients that are the irreducible factors of polynomials of the form $P_k(x) = x^k - 1$. The polynomial $P_k(x)$ has a trivial factor, namely $x - 1$, as one sees from the factorization

$$P_k(x) = x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + x^2 + x + 1)$$

For some values of k, the polynomial $P_k(x)$ factors still further into polynomials with integer coefficients. For example,

$$P_4(x) = x^4 - 1 = (x-1)(x^3 + x^2 + x + 1) = (x-1)(x+1)(x^2+1)$$

However, if $k = p$ is *prime*, then $P_k(x)$ does not factor further into polynomials with integer coefficients. That is, the polynomial $\Phi_p(x)$ given by

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

does not factor into polynomials with integer coefficients, and is therefore a cyclotomic polynomial. For concreteness, in this section we'll restrict our attention to the specific cyclotomic polynomial

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

Just as the prime factors of integers of the form $P(n) = n^2 - 5$ have an elegant characterization, so do prime factors of integers of the form $\Phi_5(n)$. Below, I've provided a table with some relevant data:

n	$\Phi_5(n)$	Factorization
1	5	5
2	31	31
3	121	11^2
4	341	$11 \cdot 31$
5	781	$11 \cdot 71$
6	1555	$5 \cdot 311$
7	2801	2801
8	4681	$31 \cdot 151$
9	7381	$11^2 \cdot 61$
10	11111	$41 \cdot 271$
11	16105	$5 \cdot 3221$
12	22621	22621
13	30941	30941
14	41371	$11 \cdot 3761$
15	406901	$11 \cdot 4931$

Aside from 5, the prime factors that appear in the table above all have final digit 1. Because the function $\Phi_5(n)$ grows rapidly with n, the prime factors of its values can be quite large even for small values of n, and so it's difficult to tell from the initial data whether *all* prime numbers with final digit 1 are prime factors of numbers of the

form $\Phi_5(n)$. However, it is not unreasonable to make

Conjecture 2: The prime factors of numbers of the form of $\Phi_5(n)$ are precisely 5 and those prime numbers with final digit 1.

which, in view of the last paragraph of Section 1, is equivalent to

Conjecture 2′: The prime factors of numbers of the form of $\Phi_5(n)$ are precisely 5 and those prime numbers that leave remainder 1 upon division by 5.

This conjecture is in fact true. Thus, the characterization of prime factors of integers of the form $\Phi_5(n)$ is in some sense similar in form to the characterization of the prime factors of integers of the form $P(n) = n^2 - 5$. However, the characterization for $\Phi_5(n)$ is easier to prove than the characterization for $P(n) = n^2 - 5$.

We refer to Conjecture 2′ as "weak cyclotomic reciprocity for $\Phi_5(n)$." It turns out that a refinement of Conjecture 2′ called "strong cyclotomic reciprocity for $\Phi_5(x)$" implies quadratic reciprocity for $P(x) = x^2 - 5$, so that proving the former gives road toward proving the latter. In fact, even weak cyclotomic reciprocity implies for each prime that leaves remainder 1 upon division by 5 divides $P(n) = n^2 - 5$ for some n.

3. Proof of a case of cyclotomic reciprocity (Part 1)

We now describe the beginning of the proof of Conjecture 2′. Let $q \neq 5$ be a prime. Recall that:

$$P_5(x) = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)\Phi_5(x)$$

In this paragraph we suppose that that q divides $P_5(n)$. Under this assumption, q divides $(n-1)\Phi_5(n)$. By unique prime factorization, if a prime divides a product, then it divides one of the factors. So if q does not divide $n-1$, then q divides $\Phi_5(n)$. In the other direction, if q divides $n-1$, then n leaves remainder 1 on division by q, so $\Phi_5(n)$ leaves remainder 5 upon division by q, so $\Phi_5(n)$ is not divisible by q.

Thus, q divides $\Phi_5(n)$ if and only if each of the following hold

(1) q divides $P_5(n)$
(2) q does not divide $n-1$

Now, q divides $P_5(n)$ if and only the remainder of n^5 upon division by q is 1, and q divides $(n-1)$ if and only if the remainder of n upon division by q is 1. So we have:

Observation: A prime $q \neq 5$ divides a number of the form $\Phi_5(n)$ if and only if n^5 leaves a remainder of 1 upon division by q and n does not leave a remainder of 1 upon division by q.

We'll use the Observation to prove Conjecture 2′. First, we need to build up knowledge of the multiplicative properties of remainders upon division by q, and in particular, knowledge of remainders of perfect powers upon division by q. We'll do this in Sections 4-6, and return to $\Phi_5(n)$ and Conjecture 2′ in Section 7.

4. The multiplicative group $(\mathrm{mod}\, q)$

Let q be a prime, and denote the integers by $\mathbb{Z}$. In the study of remainders of integers upon division by q, it is natural to consider two integers to be equivalent if they differ by a multiple of q, because if they differ by a multiple of q, then they have the same remainder upon division by q.

This equivalence relation partitions $\mathbb{Z}$ into q equivalence classes corresponding to the possible remainders upon division by q. For example, if $q = 7$ then the seven equivalence classes are those integers that leave remainder r on division by 7 for each $r \in \{0, 1, 2, 3, 4, 5, 6\}$. We denote the set of equivalence classes by $\mathbb{Z}/q\mathbb{Z}$. We write $n \equiv m \,(\mathrm{mod}\, q)$ to indicate that n and m are in the same equivalence class, and refer to the equivalence classes as "elements $(\mathrm{mod}\, q)$."

The multiplication law for $\mathbb{Z}$ induces a multiplication law on $\mathbb{Z}/q\mathbb{Z}$ as follows: the product of two elements r and s of $\mathbb{Z}/q\mathbb{Z}$ is defined by the law "pick an integer with remainder r and an integer with remainder s, multiply them together, and then take the remainder of the result." For example, taking $q = 7$, the product of 3 and 4 in $\mathbb{Z}/7\mathbb{Z}$ can be computed as the remainder of $3 \cdot 4 = 12$ upon division by 7, which is $5 \in \mathbb{Z}/7\mathbb{Z}$. One can check that the definition of multiplication is independent of the choice of integers with remainder r and with remainder s, so that multiplication of elements of $\mathbb{Z}/q\mathbb{Z}$ is well-defined. Addition of elements of $\mathbb{Z}/q\mathbb{Z}$ is defined similarly, and one can check that it is well-defined.

Multiplying an element of $\mathbb{Z}/q\mathbb{Z}$ by '1' leaves it invariant, so we call '1' the multiplicative identity of $\mathbb{Z}/q\mathbb{Z}$. If m and n satisfy $mn \equiv 1 \,(\mathrm{mod}\, q)$ then we call n the multiplicative inverse of m.

If m is a multiple of q then so is mn, so we have $0 \cdot n \equiv 0 \,(\mathrm{mod}\, q)$ for every n. In particular, 0 has no multiplicative inverse $(\mathrm{mod}\, q)$.

We write $(\mathbb{Z}/q\mathbb{Z})^*$ for set of nonzero elements of $\mathbb{Z}/q\mathbb{Z}$, endowed with the operation of multiplication. A fundamental fact is that elements of $(\mathbb{Z}/q\mathbb{Z})^*$ have multiplicative inverses. We will not prove this fact, as doing so would lead us too far afield,

but in Section 5 we place it in context by showing it to be equivalent to unique prime factorization.

5. Multiplicative inverses $(\mathrm{mod}\, q)$ and unique prime factorization

Here we show that the existence of multiplicative inverses of elements of $(\mathbb{Z}/q\mathbb{Z})^*$ for q prime is equivalent to unique prime factorization.

Proof: Let $m \in (\mathbb{Z}/q\mathbb{Z})^*$ be given. Multiplication by m defines a function $f_m(a) = ma$ from $(\mathbb{Z}/q\mathbb{Z})^*$ to itself. If f_m is a one-to-one correspondence, then f_m takes n to 1 for some n, and this n is the inverse of m. So to show the existence of multiplicative inverses, it suffices to show that the function f_m is a one-to-one correspondence.

A function from a finite set to itself is a one-to-one correspondence if and only if it takes distinct elements to distinct elements. But unique prime factorization implies that this is true of f_m, as follows:

Suppose that $mk \equiv mn \,(\mathrm{mod}\, q)$. Then $m(k-n) \equiv 0 \,(\mathrm{mod}\, q)$ so that q divides the product on the left. According to unique prime factorization, q divides one of the factors. By hypothesis, q does not divide m. So $k - n \equiv 0 \,(\mathrm{mod}\, q)$, which is the same as $k \equiv n \,(\mathrm{mod}\, q)$. So if two elements of $(\mathbb{Z}/q\mathbb{Z})^*$ have the same image under f_m, they must be the same. Thus, the function f_m is a one-to-one correspondence. So unique prime factorization implies the existence of multiplicative inverses $(\mathrm{mod}\, q)$.

The steps of the above proof are reversible, so the existence of multiplicative inverses in $(\mathbb{Z}/q\mathbb{Z})^*$ implies that if q divides a product then it divides one of the factors. But this last statement implies unique prime factorization, so the proof is complete. ■

In fact, unique prime factorization is commonly proved by utilizing the above equivalence and establishing the existence of multiplicative inverses via the *Euclidean algorithm*, which we will not describe here.

6. Perfect powers $(\mathrm{mod}\, q)$

Because of the appearance of a perfect 5^{th} power in the observation of Section 3, it is natural to study perfect powers of elements of $(\mathbb{Z}/q\mathbb{Z})^*$. Because $(\mathbb{Z}/q\mathbb{Z})^*$ is finite, if $a \in (\mathbb{Z}/q\mathbb{Z})^*$ then the sequence $a^g \,(\mathrm{mod}\, q)$ for $g = 1, 2, 3, \ldots$ cycles.

Define the *order* 'j' of an element a to be the first positive value of g for which $a^g \equiv 1 \,(\mathrm{mod}\, q)$. There is a uniform constraint on the possible values of j: no matter

what a is, j must divide $q-1$. This is sometimes known as *Fermat's little theorem.*

> **Proof:** Let H be the set of powers of a. Then H consists of j elements.
>
> Consider two elements m and n of $(\mathbb{Z}/q\mathbb{Z})^*$ to be equivalent if $mh = n$ for some $h \in H$. In other words, consider m and n to be equivalent if they differ (multiplicatively) by an element of H. Each of the $q-1$ elements of $(\mathbb{Z}/q\mathbb{Z})^*$ falls into exactly one of the resulting equivalence class. Let $g_1, g_2, \ldots g_m$ be representatives of the equivalence classes.
>
> For each i, the function $f_{g_i^{-1}}$ defined by multiplication by g_i^{-1} sends the equivalence class corresponding to g_i to H. As mentioned in the discussion of multiplicative inverses, the function $f_{g_i^{-1}}$ is a one-to-one correspondence. So the number of elements of the equivalence class of g_i is equal to the number of elements of H $(= j)$.
>
> Since this holds for each i, we have $jm = q-1$, so that j divides $q-1$, as claimed. ■

Fermat's little theorem has a converse: given a prime q, the above condition on j is the *only* condition on j that's holds for all a. Putting Fermat's little theorem together with its converse, we have:

> **Theorem A:** If q is a prime, then there is an element of $(\mathbb{Z}/q\mathbb{Z})^*$ of order j if and only if j divides $q-1$.

To prove the converse of Fermat's little theorem, it suffices to show that it's true for $j = q-1$, because if a has order $q-1$ and j' divides $q-1$ then $a^{\frac{q-1}{j'}}$ has order j'.

An element of $(\mathbb{Z}/q\mathbb{Z})^*$ that has order $q-1$ is called a *primitive root* $(\mathrm{mod}\, q)$. It is a fundamental fact that primitive roots $(\mathrm{mod}\, q)$ exist for every prime q. To prove the existence of primitive roots $(\mathrm{mod}\, q)$, we need a lemma:

> **Lemma:** If j divides $q-1$ then $x^j - 1 = 0$ has exactly j roots.
>
> **Proof:** Write $q - 1 = jm$. We have the factorization
>
> $$x^{q-1} - 1 = (x^j)^m - 1 = (x^j - 1)((x^j)^{m-1} + (x^j)^{m-2} + \ldots + x^j + 1)$$
>
> A polynomial of degree n can factor into at most n linear factors. A polynomial can have no more roots than it has linear factors. So the first factor on the right has at most j roots $(\mathrm{mod}\, q)$ and the second

factor on the right has at most $j(m-1)$ roots $(\mathrm{mod}\, q)$.

By Fermat's little theorem, all $q-1$ elements of $(\mathbb{Z}/q\mathbb{Z})^*$ are roots of the polynomial on the left, so the polynomial on the left has $q-1$ roots $(\mathrm{mod}\, q)$. So the product on the right has $q-1$ roots $(\mathrm{mod}\, q)$.

If the first factor on the right had fewer than j roots, then the total number of roots polynomial on the right hand side would be smaller than the sum of the degrees of the two factors, which is $j + j(m-1) = jm = q-1$. So first factor has exactly j roots, as claimed. ■

Now we can prove the existence of primitive roots $(\mathrm{mod}\, q)$.

Proof: Let $\ell_1^{e_1} \cdots \ell_t^{e_t}$ be the prime factorization of $q-1$.

If two elements have orders r and s, where r and s are relatively prime, then their product has order rs. (To convince yourself of this, consider the case where $r = 3$ and $s = 5$, and the case where $r = 3$ and $s = 6$).

In view of this, it suffices to show that for each i, there is an element a_i of order $\ell_i^{e_i}$. For if there are such elements, then $a_1 a_2 \cdots a_t$ has order $q-1$.

An element has order $\ell_i^{e_i}$ if and only if its order divides $\ell_i^{e_i}$ and does not divide $\ell_i^{e_i-1}$. We show that there is an element of this type.

The elements of $(\mathbb{Z}/q\mathbb{Z})^*$ satisfying $x^{\ell_i^{e_i}} - 1 \equiv 0 \,(\mathrm{mod}\, q)$ have order dividing $\ell_i^{e_i}$, and by the lemma, there are $\ell_i^{e_i}$ such elements.

Of these, the elements that have order dividing $\ell_i^{e_i-1}$ are the elements with $x^{\ell_i^{e_i-1}} - 1 \equiv 0 \,(\mathrm{mod}\, q)$, and by the lemma, there are $\ell_i^{e_i-1}$ such elements.

Because there are more elements of $(\mathbb{Z}/q\mathbb{Z})^*$ of order dividing $\ell_i^{e_i}$ than there are elements dividing $\ell_i^{e_i-1}$, there is an element of exact order $\ell_i^{e_i}$ and we're done. ■

By our remarks above, Theorem A follows.

7. Proof of a case of weak cyclotomic reciprocity (Part 2)

With the material from Sections 4-6 in hand, it's easy to prove Conjecture 2′ of Section 2. Recall that the conjecture states that those primes $q \neq 5$ that divide

numbers of the form $\Phi_5(n)$ are precisely those $q \equiv 1 \pmod 5$.

> **Proof:** By the observation from Section 3, characterizing the prime divisors of numbers of the form $\Phi_5(n)$ is the same as characterizing the primes such that there is an $n \not\equiv 1 \pmod q$ with $n^5 \equiv 1 \pmod q$.
>
> These primes are precisely those for which $(\mathbb{Z}/q\mathbb{Z})^*$ has an element of order 5.
>
> By Theorem A, a necessary and sufficient condition for $(\mathbb{Z}/q\mathbb{Z})^*$ to have an element of order 5 is that 5 divides $q-1$, and this is the same as $q \equiv 1 \pmod 5$. Conjecture $2'$ follows. ■

The same argument shows that the prime divisors q of numbers of the form $\Phi_p(n)$ where

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

other than $q = p$ are precisely those primes with $q \equiv 1 \pmod p$.

8. The general statement of weak cyclotomic reciprocity

Before returning to quadratic reciprocity, we flesh out our discussion of weak cyclotomic reciprocity, giving a general statement. In Section 2 we made reference to polynomials that are factors of polynomials of the form $P_k(x) = x^k - 1$. We remarked that $x - 1$ is always a factor, and that for $n = p$ where p is prime, the remaining factor $\Phi_p(x)$ does not factor further. We now discuss the factors of $P_k(x)$ for arbitrary k.

In general, if k' divides k then $P_{k'}(x)$ divides $P_k(x)$, so a factor of $P_{k'}(x)$ divides $P_k(x)$. The k^{th} cyclotomic polynomial, denoted by $\Phi_k(x)$, is defined to be the end result of dividing $P_k(x)$ by each irreducible factor of a polynomial of the form $P_{k'}(x)$ for which k' is a proper divisor of k. For $k = p$ prime, this agrees with our former definition of $\Phi_p(x)$. Below, we've given the polynomials $\Phi_k(x)$ for the first few composite values of k:

$\Phi_4(x) = x^2 + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_8(x) = x^4 + 1$
$\Phi_9(x) = x^6 + x^3 + 1$
$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
$\Phi_{12}(x) = x^4 - x^2 + 1$

The general statement of weak cyclotomic reciprocity is:

Weak cyclotomic reciprocity: Let k be given. The prime numbers q that divide numbers of the form $\Phi_k(n)$ that do not divide k are precisely those with $q \equiv 1 \pmod{k}$.

In Section 7 we proved the case where k is prime. The proof of the general statement of weak cyclotomic reciprocity proceeds along similar lines. However, we have not yet developed the theory to prove the general statement, and so will postpone its proof to a future set of notes.

9. The deduction of quadratic reciprocity from cyclotomic reciprocity

As commented in Section 2, the strong reciprocity law for $\Phi_5(x)$ implies the reciprocity law for $P(x) = x^2 - 5$.

Let c be a nonsquare integer. There are infinitely many values of c for which the strong reciprocity law for $\Phi_c(x)$ implies the reciprocity law for $P(x) = x^2 - c$. The strong reciprocity law for $\Phi_{4c}(x)$ *always* implies the reciprocity law for $P(x) = x^2 - c$.

We remark in passing that the weak reciprocity law for $\Phi_{4c}(x)$ implies that those primes $q \equiv 1 \pmod{c}$ are factors of numbers of the form $P(n) = n^2 - c$. However, we need the *strong* reciprocity law to characterize the *other* primes that are factors of numbers of the form $P(n) = n^2 - c$.

The deduction of the reciprocity law of $P(x) = x^2 - c$ from the strong reciprocity law for $\Phi_{4c}(x)$ requires a deep study of the (complex) roots of $\Phi_{4c}(x)$. In particular, it uses highly nonobvious fact that the roots of $P(x)$ can be written in terms of the roots of $\Phi_{4c}(x)$. We'll state the fact for $c = 5$ without proof. Let ζ be a root of

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

Then

$$(\zeta + \zeta^4 - \zeta^2 - \zeta^3)^2 = 5$$

Relationships of this type were first discovered by Gauss in the late 1700's, and he used them derive quadratic reciprocity from strong cyclotomic reciprocity.

Gauss's proof was clarified and put into perfect form in the course of the development of algebraic number theory by Évariste Galois, Ernst Kummer, Leopold Kronecker, Richard Dedekind and David Hilbert, between 1820-1900. We will describe this proof in a future set of notes.

10. Higher reciprocity laws

A *reciprocity law* can, at least initially, be thought of as a characterization of the prime factors of numbers of the form $P(n)$, where P is a polynomial with integer coefficients. Having found a reciprocity law for quadratic polynomials, it is natural to search for reciprocity laws for higher degree polynomials. The cyclotomic polynomials are easily understood, so one considers higher degree polynomials that are not cyclotomic.

Gauss considered the cases $P(x) = x^3 - c$ and $P(x) = x^4 - c$, where c is an integer that is not a perfect power. In these cases, there is no direct connection with cyclotomic reciprocity, because in contrast with the quadratic polynomials, the roots of these polynomials cannot be expressed in terms of the roots of cyclotomic polynomials alone.

Years after writing *Disquisitiones Arithmeticae*, Gauss wrote:

> *The theory of quadratic residues can be reduced to the most beautiful jewel among the fundamental theorems of higher arithmetic, which, as is known, were first discovered easily by inductive methods and then were proved in so many ways that nothing remains to be desired. However, the theory of cubic and biquadratic residues is more difficult by far. In 1805, as we began to investigate these, except for the first results which gave several special theorems that stand out both because of their simplicity and because of the difficulty of their proofs, we soon recognized that the principles of arithmetic which were usable until then were in no way sufficient to build a general theory. Rather such a theory necessarily required an infinite enlargement to some extent of the field of higher arithmetic . . .*

Though the patterns are more subtle in these cases, they are no less elegant. The patterns become still more subtle when one broadens one's consideration to arbitrary polynomials, particularly for those polynomials of degree 5 and higher that are not of very special forms. In *Representation Theory: Its Rise and Its Role in Number Theory*, Robert Langlands wrote:[2]

[2]Quotation lightly edited for context.

> *Another example, the reasons for whose choice will be explained later, is*
>
> $$P(x) = x^5 + 10x^3 - 10x^2 + 35x - 18$$
>
> *The list of its prime factors of its values begins 2063, 2213, 2953, 3631, ... This list can be continued indefinitely, but it is doubtful that even the most perspicacious and experienced mathematician would detect any regularity. It is nonetheless there.*

The study of set of prime factors of such a given polynomial falls under the rubric of the *Langlands' Program*, which, among many other things, provides a characterization of the set of prime factors of numbers of the form $P(n)$ when P is a polynomial with integer coefficients. To give a sense for the depth of the phenomena here, we give a sample theorem which we learned from Matthew Emerton.

> **Theorem:** Let $P(x) = x^3 - x - 1$. Let p be a prime. Let a_p be the coefficient of z^p in the power series defined by the product:
>
> $$f(z) = z\left[(1-z)(1-z^2)(1-z^3)\cdots\right]\left[(1-z^{23})(1-z^{46})(1-z^{69})\cdots\right]$$
>
> (Here the exponents in the third factor are the positive integer multiples of 23 in increasing order.)
>
> Then p divides a number of the form $P(n)$ if and only if $a_p = 2$ or $a_p = 0$.

The fact that quadratic reciprocity and the theorem above are special cases of the same principle is *a priori* very mysterious. This is a testament to depth and richness of reciprocity laws, and the great amount of perspective that can be gained by studying them.

11. Acknowledgements

I first learned of the statement of reciprocity laws in terms of prime factors of polynomials from Part 11 of Robert Langlands' lecture series titled *The Practice of Mathematics*.

The translation of the Gauss quotation from Section 10 is from *Mathematical Masterpieces: Further Chronicles by the Explorers* by Knoebel, et. al.

Matthew Emerton gave the theorem mentioned in Section 10 as an example in his answer to Chandan Singh Dalawat's MathOverflow question titled *Galoisian sets of prime numbers*.

I thank Paul Pollack and Timothy Gowers for helpful feedback on the exposition and content of the notes. In particular, I thank Paul Pollack for pointing out an error in an earlier version of the notes.