Some simple proofs on general reciprocity.

Jim H. Adams © 2013

We will use Fermat's little theorem to prove for odd primes the celebrated theorem of quadratic reciprocity, and extend it to odd composite numbers. We prove the corresponding results for cubic and biquadratic reciprocity, and show for matrices in the $\mathbb{D}1$ exponential algebra of [Ad14] that these results can be developed further.

In order to appeal to the widest possible audience the Legendre and Jacobi symbols do not appear in this work, and to begin with use of the mod notation has been suppressed.

Let p and q be distinct odd primes, and other lower case letters be integers. An equation (x) in section w is denoted by (x) within the section and w.(x) outside of it. '□' denotes the completion of a stage of a proof, '□→' a new idea, and '□←' a return to standard reasoning.

1. Fermat's little theorem and quadratic reciprocity.

Theorem 1.1. Fermat's little theorem states for prime p, verifiable directly for p = 2

$$x^p - x = bp. \tag{1}$$

for some unique b dependent on x.

Proof. We prove this by induction. For x = 0

$$0^p - 0 = 0p.$$

Assume (1) holds. Then for $x \to x + 1$, by the binomial theorem and the primality of p, so p does not divide any denominator

$$(x + 1)^p - (x + 1) = x^p - x + px^{p-1} + [p(p - 1)/2]x^{p-2} + ... + 1^p - 1 = bp + cp$$

for some unique c. □ (2)

Theorem 1.2. The law of quadratic reciprocity states there exists a unique n and m such that

$$(q^{(p-1)/2} - np)(p^{(q-1)/2} - mq) = (-1)^{(p-1)/2\,(q-1)/2}. \tag{3}$$

This can be rephrased using the Euclidean algorithm, that for any given y and for any r > 0 there exist unique natural numbers n and a with a < r such that y = a + nr. On putting r = p and $y = q^{(p-1)/2}$, this implies n is unique in (3) if $(q^{(p-1)/2} - np) < p$.

We will deal with squares up to equation (7), minus signs up to equation (8) and then powers up to equation (11) to establish this quadratic reciprocity theorem.

Proof. Fermat's little theorem may be rewritten from (1) as

$$x(x^{p-1} - 1) = x[(x^2)^{(p-1)/2} - 1]$$
$$= x(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = bp, \tag{4}$$

so that if x is not zero or another multiple of p, for some unique r, s and t, squares in x are of the form

$$x^{(p-1)/2} = 1 + rp \text{ if and only if } (x^2)^{(p-1)/2} = 1 + sp, \tag{5}$$

otherwise non-squares are of the form

$$x^{(p-1)/2} = -1 + tp. \text{ □} \tag{6}$$

On substituting (q – p) for x, which cannot be zero or another multiple of p, we obtain from equations (5) and (6)

$$(q - p)^{(p-1)/2} = \pm 1 + up, \qquad (7)$$

for some unique u. Less multiples of p, the $q^{(p-1)/2}$ term in the binomial expansion of (7) is ±1.

Note that:

if (p – 1)/2 is even, then $x^{(p-1)/2} = (-x)^{(p-1)/2}$,
but if (p – 1)/2 is odd, then $x^{(p-1)/2} = -(-x)^{(p-1)/2}$. (8)

Under the transformation of (q – p) to its negative, (p – q), when (p – 1)/2 is odd, on using equation (8) the sign ±1 in (7) becomes reversed, but when (p – 1)/2 is even, the sign remains the same. □

Using the binomial theorem, by taking the $(q - 1)/2^{th}$ power at the right hand side of (7), for both (p – 1)/2 and (q – 1)/2 odd

$$[(q - p)^{(p-1)/2}]^{(q-1)/2} = (\pm 1 + up)^{(q-1)/2} = \pm 1 + vp, \qquad (9)$$

for some unique v, where the ± is carried through unchanged in all expressions. Then by the remark after (7), for some unique w this is

$$q^{(p-1)/2} - wp,$$

but for (q – 1)/2 even, the analogue of (9) is

$$(\pm 1 + up)^{(q-1)/2} = +1 + vp. \ \square$$

Now $[(-1)^{(p-1)/2}]^{(q-1)/2}$ is -1 if and only if (p – 1)/2 and (q – 1)/2 are both odd.

Using equation (9) and the remark after (8), with both (p – 1)/2 and (q – 1)/2 odd there exists an n = w + v, and a similarly derived m for which

$$\begin{aligned}[(q - p)^{(p-1)/2}]^{(q-1)/2}[(p - q)^{(q-1)/2}]^{(p-1)/2} &= (q^{(p-1)/2} - np)(p^{(q-1)/2} - mq) \\ &= -1(\pm 1)^2 \\ &= (-1)^{(p-1)/2\,(q-1)/2},\end{aligned}$$

and this version of (3) also holds when (p – 1)/2 or (q – 1)/2 are even. We prove this next.

We will write x = a + np by $x \equiv a \pmod p$, and call a the *residue* (mod p). This notation will be used in conjunction with the Euclidean algorithm.

If $x \equiv x' \pmod p$ we say x and x′ are *congruent* (mod p), otherwise *incongruent* (mod p). A result we shall use is: if a general polynomial f(x) in x satisfies f(x) = x′, then the congruence

$$f(x) \equiv x' \pmod p$$

also holds.

If (p – 1)/2 is even and (q – 1)/2 is odd – the quadratic reciprocity theorem is symmetrical with respect to p and q, so this also holds when (p – 1)/2 is odd and (q – 1)/2 is even, then

$$[(q - p)^{(p-1)/2}]^{(q-1)/2} \equiv 1 \pmod p,$$

which equates to

$$\begin{aligned}(q^{(p-1)/2})^{(q-1)/2} &\equiv 1 \pmod p \\ &\equiv q^{(p-1)/2} \pmod p, \qquad (10)\end{aligned}$$

so by the Euclidean algorithm there exists an n with

$$q^{(p-1)/2} - np = 1,$$

whereas

$$[-(q-p)^{(q-1)/2}]^{(p-1)/2} \equiv 1 \pmod{q},$$
$$\equiv p^{(q-1)/2} \pmod{q}, \qquad (11)$$

and the product of (10) and (11) is in this particular circumstance $[1 \pmod p][1 \pmod q] = 1$.

If both $(p-1)/2$ and $(q-1)/2$ are even, clearly the product of (10) and (11) again has leading terms 1. □

2. Euler's totient formula [Ma1886].

Let t be any positive integer, and let the totient $\varphi(t)$ denote the number of positive integers, 1 included, which are coprime to t and not greater than t.

By definition $\varphi(1) = 1$. Also if p is a prime number

$$\varphi(p) = p - 1.$$

Next suppose t composite, and let p, q, r, s, ... be the different primes which divide t.

Consider the series of integers, 1, 2, 3, ... t. Of these the following are multiples of p:

$$p, 2p, 3p, \ldots (t/p).p,$$

(t/p in all).

Write these down with the sign +. Similarly, write down all the multiples of q, r, s, ... each with the sign +.

In the same series there are t/(pq) multiples of pq. Write these down with the sign –: and do the same with all the multiples of pr, ps, qr, ... (taking all the products of p, q, r, s, ... two at a time).

Next write down all the multiples of the triple products pqr, pqs, ... each with the sign +, and so on, until at last we come to the multiples of pqrs... with sign $(-1)^{k-1}$, k being the number of different primes.

Now take any number θ which is not greater than t and not coprime to it. It will involve in its composition a certain number (λ say) of the different primes p, q, r, ... How many times will it occur among the multiples already written down?

By the binomial theorem, the number of combinations of λ things taken u at a time is

$$\lambda!/[u!(\lambda - u)!].$$

Evidently, taking its appearances in the order of the sets of multiples, θ will occur for λ times, the binomial coefficient, for u = 1 with the sign +, then for $\lambda(\lambda-1)/2$ times for u = 2 with the sign –, then $\lambda(\lambda-1)(\lambda-3)/3!$ times for u = 3 with the sign +, and so on.

If then we take the algebraic sum of all the sets, we have θ occurring with a coefficient

$$\lambda - \lambda(\lambda-1)/2! + \lambda(\lambda-1)(\lambda-3)/3! - \ldots = 1 - (1-1)^{\lambda} = 1.$$

Thus the algebraic sum in question is the sum of all positive integers not greater than t and not coprime to it. Now the *number* of these integers is equal to the excess of the number of positive terms in the whole sum, as originally written, above the number of negative terms:

$$t\{(1/p + 1/q + 1/r + ...) - (1/(pq) + 1/(pr) + 1/(qr) + ...) + (1/(pqr) + 1/(pqs) + ...) - ... + (-1)^{k-1}.1/(pqrs ...)\}.$$

Subtracting this from t, we have finally

$$\varphi(t) = t(1 - 1/p)(1 - 1/q)(1 - 1/r) ... \square \qquad (1)$$

Corollary 2.1. If t is odd, φ(t) is even. □

3. The Frobenius automorphism, Fermat's and Euler's theorems.

We now give a second proof of Fermat's little theorem (theorem 3.1), then Euler's extension from this to composite numbers. It uses what is known as the Frobenius automorphism, but it is evident in the much earlier work of Galois.

For prime p the bijective mapping, called the Frobenius automorphism

$$x \pmod p \leftrightarrow kx \pmod p,$$

for k not a multiple of p, permutes the elements k = (1, 2, ... x). This was known to Galois, and is essentially a statement of the Euclidean algorithm. The Frobenius automorphism is commutative: $k_1k_2 = k_2k_1$. In detail, if there are two codomains of the above function for domains x and x′ such that kx = kx′, or otherwise kx ≠ kx′, then

$$x \equiv x' \pmod p, \text{ or respectively } kx \neq kx' \pmod p,$$

and since x spans all 0, 1, ... (p – 1), so therefore do the kx. □

Theorem 3.1. The numbers x, 2x, 3x, ... (p – 1)x are all incongruent to each other (mod p). Their least positive residues are therefore 1, 2, 3, ... (p – 1) in a certain order. Consequently

$$x.2x.3x ... (p-1)x \equiv 1.2.3 ... (p-1) \pmod p,$$

and on dividing both sides by (p – 1)!, which is coprime to p,

$$x^{p-1} \equiv 1 \pmod p,$$

when x is not congruent to p. □

We are now in a position to prove Euler's totient theorem.

Theorem 3.2. Let t be prime or composite, then

$$\varphi(t)[x^{\varphi(t)+1} - x] \equiv 0 \pmod t. \qquad (1)$$

Proof. Consider first the case when x is coprime to t′. If α, β, γ, ... λ are the φ(t′) numbers which are prime to t′ and less than it, the products xα, xβ, xγ, ... xλ are all coprime to t′; moreover we have seen no two of them are congruent (mod t′). Hence the products xα, xβ, xγ, ... xλ are congruent to α, β, γ, ... λ in a different order, and therefore

$$x\alpha.x\beta.x\gamma ... x\lambda = \alpha.\beta.\gamma ... \lambda.$$

Dividing by α.β.γ ... λ, which is coprime to t′, we obtain

$$x^{\varphi(t')} - 1 \equiv 0 \pmod{t'},$$

when x is coprime to t′. In the case when x is not coprime to t″, derived from formula 2.(1), with t = t′t″ and only t′ coprime to x, φ(t″)x ≡ 0 (mod t″). Then on using φ(t) = φ(t′)φ(t″) and (mod t) = (mod t′)(mod t″), theorem 3.2 is obtained from

$$(x^{\varphi(t)} - 1) = (x^{\varphi(t')} - 1)(x^{\varphi(t) - \varphi(t')} + x^{\varphi(t) - 2\varphi(t')} + ... + 1). \square$$

4. Totient quadratic reciprocity.

Extending section 1 now to totients, Euler's theorem may be rewritten from 3.(1) as

$$\varphi(t)[x(x^{\varphi(t)} - 1)] \equiv \varphi(t)x[(x^2)^{\varphi(t)/2} - 1] \equiv 0 \pmod t$$
$$\equiv \varphi(t)x(x^{\varphi(t)/2} - 1)(x^{\varphi(t)/2} + 1) \pmod t, \quad (1)$$

so that non $x \equiv 0 \pmod t$ squares in x are of the form

$$\varphi(t)x^{\varphi(t)/2} \equiv \varphi(t) \pmod t \text{ if and only if } \varphi(t)(x^2)^{\varphi(t)/2} \equiv \varphi(t) \pmod t, \quad (2)$$

and non-squares are of the form

$$\varphi(t)x^{\varphi(t)/2} \equiv -\varphi(t) \pmod t. \ \square \quad (3)$$

Let t and u be possibly composite numbers. Then on substituting $(t - u)$ for x, we obtain from (2) and (3)

$$\varphi(u)(t - u)^{\varphi(u)/2} \equiv \pm\varphi(u) \pmod u. \quad (4)$$

The binomial expression on the left of (4) contains

$$t^{\varphi(u)/2} + [\varphi(u)/2]t^{[\varphi(u)/2]-1}(-u) + \{[\varphi(u)/2][(\varphi(u)/2) - 1]/2\}t^{[\varphi(u)/2]-2}(-u)^2 + ... + (-u)^{\varphi(u)/2},$$

where each coefficient is a natural number, and thus (4) is

$$\varphi(u)t^{\varphi(u)/2} \equiv \pm\varphi(u) \pmod u. \quad (5)$$

Considering also $(u - t)^{\varphi(t)/2}$, if $\varphi(u)/2$ and $\varphi(t)/2$ are odd, taking both powers we have

$$\varphi(t)^{\varphi(u)/2}\varphi(u)^{\varphi(t)/2}[t^{\varphi(u)/2} \pmod u][u^{\varphi(t)/2} \pmod t] = [\varphi(t)^{\varphi(u)/2}\varphi(u)^{\varphi(t)/2}](-1)^{\varphi(u)\,\varphi(t)/4}, \quad (6)$$

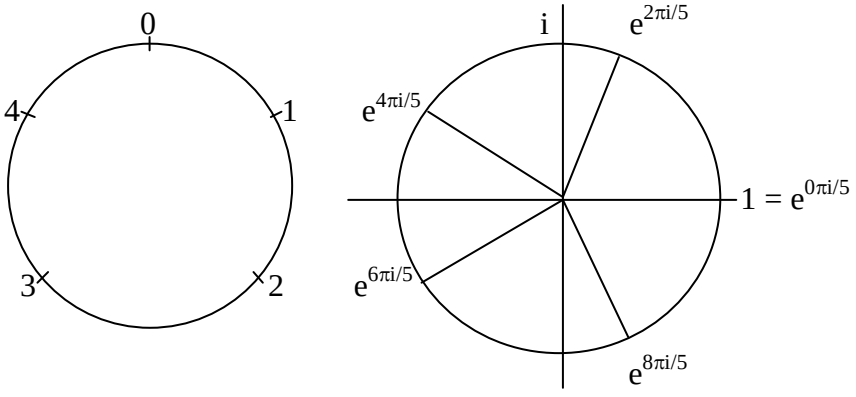
and as in section 1, we also maintain the above totient quadratic reciprocity when $\varphi(u)/2$, $\varphi(t)/2$ or both are even. $\square$

5. Quadratic Eisenstein representations.

Theorem 5.1. There is a bijection for fixed r

$$x \pmod p \leftrightarrow e^{r + (2\pi i x/p)},$$

which can be depicted in the example diagram for p = 5:



x (mod 5) complex (Argand) diagram with unit radius

Figure 5.1.

The clock, or congruence, arithmetic on the left starts from 0 at the top and proceeds clockwise. The corresponding complex diagram on the right starts from $1 = e^{0\pi i/5}$ depicted on the horizontal axis, and proceeds anticlockwise. $\square$

□→

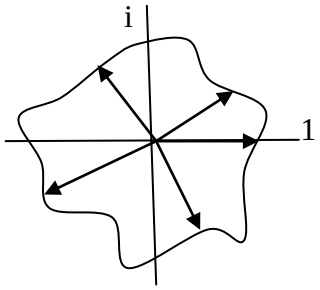


Figure 5.2.

We may generalise the complex diagram depicting $e^{2\pi ix/p}$ of figure 5.1 to the radii in polar coordinates of figure 5.2 above. The radial vectors from the centre are of magnitude r_x, with r_0 horizontal, where x varies from $-(p-1)/2$ to $+(p-1)/2$.

In order to represent the features of quadratic reciprocity theorems, we partition the r_x to belong to either a positive or a negative equivalence class, and specify that the r_x occupy the domain of functions f with target $f(r_0) = 0$, $f(r_1)$ to $f(r_{(p-1)/2})$ positive and $f(r_{-(p-1)/2})$ to $f(r_{-1})$ negative, together with the symmetry requirement that every $f(r_x)$ in the positive class is matched with a $f(r_{-x})$ in the negative class of equal magnitude and opposite sign. This is the *quadratic Eisenstein representation*.

We extend the Frobenius automorphism to apply to the positive equivalence class of the $f(r_x)$. Under multiplication by k there is a bijective mapping

$$f(r_x) \leftrightarrow f(r_{kx}) = -f(r_{-kx}) \leftrightarrow \pm f(r_y) \pmod p,$$

in which the set $\{f(r_x)\}$ is mapped to the set $\{\pm f(r_y)\}$, where $f(r_x)$ and $f(r_{-x}) = -f(r_x)$ are distinct and $f(r_{kx}) \neq f(r_{-kx})$, the reasoning being similar to the standard Frobenius permutation.

Applying the Frobenius automorphism to the subset

$$(1, 2, \ldots (p-1)/2) \pmod p \leftrightarrow (k, 2k, \ldots (p-1)k/2) \pmod p$$

we have a corresponding map on subscripted variables

$$(f(r_1), f(r_2), \ldots f(r_{(p-1)/2})) \pmod p \leftrightarrow (f(r_k), f(r_{2k}) \ldots f(r_{(p-1)k/2})) \pmod p,$$

and a ± map of permuted products, the codomain of $f(r_j)$ being the codomain of $\pm f(r_{jk})$:

$$\prod_{j=1}^{(p-1)/2}[f(r_j)] \pmod p \leftrightarrow \prod_{j=1}^{(p-1)/2}[f(r_{jk})] \pmod p. \ \square\leftarrow$$

Since the Frobenius automorphism captures the structure of the Euler totient formula, the quadratic Eisenstein representation applies to the totient quadratic reciprocity formula of section 4. In particular on extending from (mod p) to a composite (mod u), we have the equality below with the multiple product on the right

$$t^{\varphi(u)/2} \pmod u = \prod_{j=1}^{\varphi(u)/2}[f(r_{tj})/f(r_j)].$$

We may now select a model representing $t^{\varphi(u)/2}$. Since $\sin 0\pi = 0$ and $\sin 2\pi t/(\varphi(u) + 1)$ is positive from values $t = 1$ to $\varphi(u)/2$, and negative from values $t = \varphi(u)/2 + 1$ to $\varphi(u)$, this satisfies our requirements and

$$t^{\varphi(u)/2} \pmod u = \prod_{j=1}^{\varphi(u)/2}[\sin 2\pi tj/(\varphi(u) + 1)]/[\sin 2\pi j/(\varphi(u) + 1)], \qquad (1)$$

or using $e^{i\psi} = \cos\psi + i\sin\psi$

$$t^{\varphi(u)/2} \pmod u = \prod_{j=1}^{\varphi(u)/2}[e^{i2\pi tj/(\varphi(u)+1)} - e^{-i2\pi tj/(\varphi(u)+1)}]/[e^{i2\pi j/(\varphi(u)+1)} - e^{-i2\pi j/(\varphi(u)+1)}]. \ \square$$

6. Totient general reciprocity.

We will now specialise to the circumstances where $\varphi(t)/n$ exists (mod t) – this is always the case for $n \neq mt$ and t prime – and write Euler's theorem as

$$\varphi(t)x(x^{\varphi(t)} - 1) \equiv \varphi(t)x\prod_{j=1}^{n}[x^{\varphi(t)/n} - \omega_n{}^j] \equiv 0 \text{ (mod t)}, \quad (1)$$

where $\omega_n = e^{2\pi i/n}$ is an nth root of unity.

We can prove that with h constant, the product

$$0 = (1 - 1) = \prod_{j=1}^{n}(\omega_n{}^h - \omega_n{}^j), \quad (2)$$

since if it were not zero, and were represented by the little arrow in the example Argand diagram below

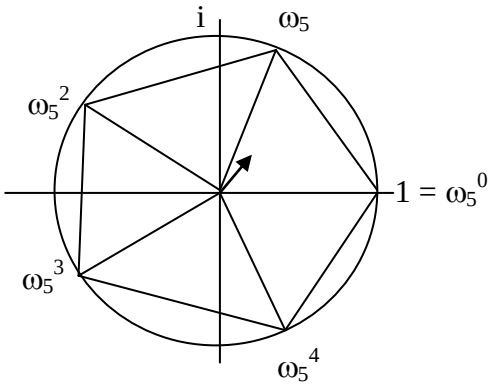


Figure 6.1.

Argand root diagram

then under the transformation $\omega_n{}^j \rightarrow \omega_n{}^{j+1}$, which leaves the product invariant, the little arrow would rotate, therefore it must be the zero vector. Moreover, (2) holds (mod t), so if $x \neq 0$, then (1) holds (mod t), and it is valid as well when $x \equiv 0$ (mod t). □

For $n \leq 4$ expression (1) exists in a unique factorisation domain, but for $n > 4$ the expression $\prod_{j=1}^{n}[x^{\varphi(t)/n} - \omega_n{}^j]$ does not uniquely factorise in general. However, this is irrelevant, since the fundamental theorem of algebra specifies that factorisation in (1) is unique (mod t) up to permutation of the roots when the product in (1) (mod t) is equivalent to zero. □

In a parallel argument to section 4, under the stipulations now given that $\varphi(t)/n$ (mod t) and $\varphi(u)/n$ (mod u) exist, we derive

$$\varphi(t)^{\varphi(u)/n}\varphi(u)^{\varphi(t)/n}[t^{\varphi(u)/n} \text{ (mod u)}][u^{\varphi(t)/n} \text{ (mod t)}] = [\varphi(t)^{\varphi(u)/n}\varphi(u)^{\varphi(t)/n}](-1)^{\varphi(u)/n\ \varphi(t)/n}. \square \quad (3)$$

7. General Eisenstein representations.

Since by assumption $\varphi(u)/n$ (mod u) exists, we may form the set

$$\{1, 2, \ldots \varphi(u)/n, \ldots \omega_n{}^s, 2\omega_n{}^s, \ldots \varphi(u)\omega_n{}^s/n, \ldots \omega_n{}^{n-1}, 2\omega_n{}^{n-1}, \ldots \varphi(u)\omega_n{}^{n-1}/n\},$$

where elements may have no inverse (mod u). We generalise the quadratic Frobenius automorphism to apply to this set, so that we obtain the general Frobenius endomorphism

$$\prod_{j=1}^{\varphi(u)/n}[f(r_j)] \text{ (mod u)} \rightarrow \prod_{j=1}^{\varphi(u)/n}[f(r_{jk})] \text{ (mod u)},$$

and we may search for a model of $t^{\varphi(u)/n}$ (mod u), if it exists.

For n = 4 we obtain the partition $\omega_n{}^s = 1, i, -1, -i$, corresponding to the form 6.(1)

$$\varphi(u)x(x^{\varphi(u)} - 1) \equiv \varphi(u)x[x^{\varphi(u)/4} - 1][x^{\varphi(u)/4} - i][x^{\varphi(u)/4} + 1][x^{\varphi(u)/4} + i] \equiv 0 \text{ (mod u)}.$$

We designate by x = sn v the elliptic function of v which satisfies the differential equation

$$dx = dv.\sqrt{1 - x^4}. \quad (1)$$

The elliptic functions, a reference being [Ca1895], may be written in Gudermann notation as

$$cn\ v = \cos\psi,\ sn\ v = \sin\psi,\ dn\ v = \sqrt{1 - \kappa^2 \sin^2\psi},$$

where

$$v = \int_0^{\psi} (1 - \kappa^2 \sin^2\psi)^{-½}$$

for which expanding by the binomial theorem gives

$$(1 - \kappa^2 \sin^2\psi)^{-½} = 1 + \sum_{m=1}^{\infty} [(1.3.5. \ldots (2m - 1))/(2.4.6 \ldots 2m)](\kappa \sin\psi)^{2m}.$$

From equation (1) we have automatically

$$sn\ iv = i\ sn\ v,$$

and find four cases

$$[sn\ 2\pi tj/(\varphi(u) + 1)]/[sn\ 2\pi j/(\varphi(u) + 1)] = 1, i, -1 \text{ or } -i, \quad (2)$$

so that setting

$$t^{\varphi(u)/4} \pmod u = \prod_{j=1}^{\varphi(u)/4} [sn\ 2\pi tj/(\varphi(u) + 1)]/[sn\ 2\pi j/(\varphi(u) + 1)], \quad (3)$$

sn acts as a model for an expression of $t^{\varphi(u)/4} \pmod u$. □

To demonstrate the reciprocity law relative to cubic residues, we put in place of the differential equation (1) that of

$$dx = dv.\sqrt{1 - x^3} \text{ or } dx = dv.\sqrt{x(1 - x^3)},$$

the rest consists of considering the roots $\omega_3^2 + \omega_3 + 1 = 0$, and the remainder of the proofs are perfectly analogous. □

8. The complex algebraic Fermat and Euler theorems.

Let p be odd and x = a + bi (a Gaussian integer). If (p – 1)/2 is even, p is of the form 4k + 1 and by binomial expansion the real component is

$$a^p - a \equiv 0 \pmod p,$$

and the imaginary component is

$$(bi)^p - bi \equiv 0 \pmod p,$$

so that with (mod p) interpreted as a vector

$$x^p - x \equiv 0 \pmod p.$$

However, if (p – 1)/2 is odd, so p = 4k – 1, then

$$a^p - a \equiv 0 \pmod p,$$

but in order to retain the Fermat theorem, on the imaginary component it satisfies

$$-(bi)^p - bi \equiv 0 \pmod p,$$

that is, overall, where x* is the complex conjugate

$$x^p - x^* \equiv 0 \pmod p. \ \square$$

We can say likewise for the Euler formula, that when x = u + vi, then

$$\varphi(t)[u^{\varphi(t) + 1} - u] \equiv 0 \pmod t, \quad (1)$$

and for the imaginary component

$$\varphi(t)[v^{\varphi(t)+1} - (-1)^{\varphi(t)/2}v] \equiv 0 \pmod{t}. \quad \square \qquad (2)$$

Fractions may be obtained from inverses. When u is coprime to t, the inverse of u is

$$u^{-1} \equiv u^{\varphi(t)-1} \pmod{t},$$

but otherwise u has no inverse, since if u^{-1} existed, $\varphi(t)u \equiv 0 \pmod{t}$ would imply $\varphi(t) \equiv 0 \pmod{t}$. Similarly the inverse v^{-1}, if it exists, is

$$v^{-1} \equiv (-1)^{\varphi(t)/2}v^{(\varphi(t)-1)} \pmod{t},$$

although $v^{-1} \pmod{t}$ may not exist. More relevant, x(x*) is a scalar, call it z, so that the inverse of x is x*/z, where $z \neq 0 \pmod{t}$.

For a further discussion, see [Ad14] Ch III, on Wedderburn's little theorem. There are cases where a finite subalgebra of the complex numbers does not contain some non-zero inverses (mod t), corresponding to situations where 1/n is absent (mod t) for 1/n complex. The only case where inverses are always present is when t is prime of the form 4k – 1. □

The complex Fermat and Euler theorems also apply to algebraic numbers.

For p = 2 we have

$$i^2 = -1 \equiv 1 \pmod{2},$$

so that $i = 1 \pmod{2}$, and for n odd

$$\sqrt{n}.\sqrt{n} = n \equiv 1 \pmod{2},$$

so $\sqrt{n} \equiv 1 \pmod{2}$, and likewise $\sqrt{n} \equiv 0 \pmod{2}$ for n even is a possibility. However, another allocation is derived from

$$\sqrt{2} \equiv 1 + i \pmod{2},$$

so that

$$\sqrt{2}.\sqrt{2} = 2 \equiv 0 \equiv (1 - 1) + 2i \pmod{2}.$$

For mth roots, m odd

$$n^{1/m} \equiv n \pmod{2},$$

but (1/m), m even (mod 2), does not exist, since for example

$$1/(1 + i) = (1 - i)/[(1 + i)(1 - i)] = (1 - i)/2,$$

and $2 \equiv 0 \pmod{2}$. Nevertheless, we can apportion, m even,

$$n^{1/m} \equiv n \pmod{2},$$

so that taking roots (mod 2) has no effect on the value of n. Since forming a square (mod 2) has no effect either, this is consistent. □

When p is an odd prime, from [Ad11], section 2, there are (p – 1)/2 squares, provided $x \neq 0$, of the form $x^2 \pmod{p}$, and (p – 1)/2 non-squares (mod p).

For p = 4k – 1, so (p – 1)/2 is odd, $i^2 = -1 \equiv p - 1 \pmod{p}$. We have previously proved that if (p – 1)/2 is odd, then $x^{(p-1)/2} = -(-x)^{(p-1)/2}$, and for a square $x^{(p-1)/2} = 1$ but -1 is not. So if x here is a square, -x is not a square in integer clock arithmetic.

However, with Gaussian clock arithmetic, which has complex integer components, for the complex component i, $i^2 = -1$ is a square, so the role of non-square for the integer component becomes a square for the imaginary integer component. There are multiple representations of numbers in this congruence arithmetic, for instance as

(square)(integer) + (non-square)(integer) (mod p),

(square)(integer) + (square)(imaginary integer) (mod p),

where (square) (mod p) ≡ -(non-square) (mod p).

We have now a possible allocation of $\sqrt{n}$ (mod p) for p = 4k – 1. This is possible anyway by subtracting rp from the integer part, but here $\sqrt{n}$ is expressible in terms of integers (mod p). If n is a square (mod p), we have no problems in allocating $\sqrt{n}$ as an integer. If n is not a square (mod p), so it is of the form $\sqrt{h}$ where -h = n is a square, then this can be represented by $i\sqrt{n}$.

For (p – 1)/2 odd, that is p = 4k – 1, we will display square roots for the example p = 7

$1^{½} \equiv 1$ and 6 (mod 7)

$2^{½} \equiv 3$ and 4 (mod 7)

$3^{½} \equiv 2i$ and 5i (mod 7)

$4^{½} \equiv 2$ and 5 (mod 7)

$5^{½} \equiv 3i$ and 4i (mod 7)

$6^{½} \equiv i$ and 6i (mod 7).

Then $\sqrt{n}$ is representable in all cases and arbitrary allocations can cover the full gamut of values (mod p). □

For p = 4k + 1, we have proved that if (p – 1)/2 is even, then $x^{(p-1)/2} = (-x)^{(p-1)/2}$, and again for a square $x^{(p-1)/2} = 1$. So if x is a square, -x is also a square in this integer clock arithmetic.

This means that for (p – 1)/2 even, some values of $\sqrt{n}$ are not covered by integer values in complex algebraic arithmetic (mod p), since if ±x is not a square, nor is ±ix. This corresponds to precisely half the non-zero values (mod p). Nevertheless, we can still operate with $\sqrt{n}$ in a purely formal way, subject to the constraint $\sqrt{n}.\sqrt{n} = n$, even though $\sqrt{n}$ has not now been directly evaluated in terms of Gaussian integers (mod p).

For (p – 1)/2 even, that is p = 4k + 1, square roots for p = 13 are

$1^{½} \equiv 1$ and -1 (mod 13)

$2^{½} \equiv \sqrt{2}$ and $-\sqrt{2}$ (mod 13)

$3^{½} \equiv 4$ and -4 (mod 13)

$4^{½} \equiv 2$ and -2 (mod 13)

$5^{½} \equiv \sqrt{5}$ and $-\sqrt{5}$ (mod 13)

$6^{½} \equiv \sqrt{6}$ and $-\sqrt{6}$ (mod 13)

$7^{½} \equiv \sqrt{7}$ and $-\sqrt{7}$ (mod 13)

$8^{½} \equiv \sqrt{8}$ and $-\sqrt{8}$ (mod 13)

$9^{½} \equiv 3$ and -3 (mod 13)
$10^{½} \equiv 6$ and -6 (mod 13)
$11^{½} \equiv \sqrt{11}$ and $-\sqrt{11}$ (mod 13)
$12^{½} \equiv 5$ and -5 (mod 13).

Even in this case, for the allocation of square roots we note that $\sqrt{-n}$, $n \in \mathbb{N}$, becomes the imaginary number i, which can be accommodated in the above discussion, multiplied by $\sqrt{n}$, so if $m^{½}$ is a root (mod p) then $(p - m)^{½}i$ is also a root for $m^{½}$ (mod p), for example

$2^{½} \equiv \sqrt{2}$ and $-\sqrt{2}$ (mod 13)
$\equiv \sqrt{11}i$ and $-\sqrt{11}i$ (mod 13).

If $m^{½} \equiv \sqrt{r_m}$ (mod p) and $m'^{½} \equiv \sqrt{r'_m}$ (mod p), and if $(mm') \equiv q$ (mod p) then

$q^{½} \equiv \sqrt{r_m r'_m}$ (mod p),

and this gives many relations between roots, for example

$2^{½}7^{½} \equiv 14^{½} \equiv 1^{½} \equiv (12^{½})i \equiv 5i, -5i$ (mod 13)

so

$7^{½} \equiv \sqrt{7}, -\sqrt{7} \equiv 5i/\sqrt{2}, -5i/\sqrt{2}$ (mod 13).

In order to develop the theory for mth roots, the situation is directly analogous. For roots of unity, since $e^{i\theta} = \cos\theta + i\sin\theta$, and although in this case the trigonometric functions are not always square roots that can be directly evaluated, we can still treat $e^{i\theta}$ in a purely formal way as belonging to a congruence arithmetic.

These comments are related to aspects of class field theory.

This algebra can be extended further. A general complex number is of the form $e^{r+i\theta}$, but we might investigate the concoction $a^b e^{i\theta}$ where a and b are integers and θ is of the form $2\pi/m$, m an integer. We are then free to consider $a^b e^{i\theta}$ (mod t), where we are interested in b and θ related in some way to t.

For m = 1 we have already discussed $\varphi(t)[x^{\varphi(t)+1} - x] \equiv 0$ (mod t) or $\varphi(t)[x^{\varphi(t)+1} - x^*] \equiv 0$ (mod t), and φ(t) is not, yet, complex. Since e is transcendental, and a and b are not, we expect r to be transcendental in $a^b = e^r$. This indicates an obstruction to extending reciprocity theorems to complex arithmetic.

However, we can define congruence arithmetic not only (mod t), but also (mod $e^{i\theta}$), so that we can discuss for instance

$e^{i2n\pi/m}$ (mod $e^{i2\pi/m}$).

It is possible to multiply both these factors by natural numbers, or by rational numbers if we are not dividing by zero.

We will continue this discussion in the section on exponential algebra 𝔻1. □

9. The Euler theorem for superexponential congruence arithmetic.

We have already met in section 5 the bijection: $x \pmod p \leftrightarrow e^{r + (2\pi ix/p)}$, and so we are able to introduce congruence arithmetic in the exponential part of expressions.

Writing $e\uparrow\theta$ for e^{θ}, when x is real we obtain the easy result

$$e\uparrow[\varphi(t)x(x^{\varphi(t)} - 1)] \equiv e\uparrow 0 \equiv 1 \pmod t \equiv 0 \pmod{e\uparrow t},$$

and for a general superexponential operator, as given in [Ad13]

$$e\Uparrow[\varphi(t)x(x^{\varphi(t)} - 1)] \equiv e\Uparrow 0 \equiv 0 \pmod{e\Uparrow t}. \square$$

10. The complex and intricate Fermat and Euler theorems for ladder numbers.

$\square\rightarrow$ Ladder numbers, which are a replacement of the reals, involve infinite and infinitesimal 'rungs'. $\square\leftarrow$ These are described in [Ad13].

Let w be a ladder number with hyperinfinite and hyperinfinitesimal rungs. The cardinality of the set {w} of w is M_n, where n = 0 indicates this is countable, and we take n non-negative. Let $x \in \mathbf{L}_Z$ be ladder integers on all rungs, where these rungs are finite in number, and t be a natural number $\in \mathbb{N} \subset \mathbf{L}_Z$.

Then Euler's totient formula becomes

$$w\varphi(t)[x^{\varphi(t) + 1} - x] \equiv 0 \pmod{wt}. \qquad (1)$$

In the case where x = u + iv is complex, so that we say ladder number $x \in \mathbf{L}_C$, equation (1) continues to hold on its u component, and its modification in 8.(2) for v. $\square$

The intricate algebra of [Ad14] expresses the 2×2 noncommutative matrix

$$x = a1 + bi + c\alpha + d\phi$$

as the matrix x = a1 + JK where $J^2K^2 = -b^2 + c^2 + d^2$ and

$$J^2 = 0 \text{ or } \pm 1. \qquad (2)$$

Then for $J^2 = -1$ the algebra works under the substitution $J \rightarrow i$, and the considerations for complex x carry over to these matrices.

If we take K^2 as an integer, then we can represent $\pm K$ in the manner we have already accomplished in section 8. Further, the intricate conjugate of x is

$$x^* = a1 - bi - c\alpha - d\phi,$$

so that we can adopt equation (1) etc. in the intricate case with J replacing i. $\square$

11. The complex and intricate exponential algebra D1.

For complex powers of a real variable, we may take

$$x^{p + qi} = x^p.(x^q)^i = x^p.(x^i)^q.$$

$\square\rightarrow$ Both in the case of real and complex x we adopt the non-standard $\mathbb{D}1$ exponential algebra of [Ad14]. This algebra is not a multifunction algebra, outside of m identical complex roots $e^{r + i(\pi\theta + 2\pi m)}$. In more detail, this algebra differs from the standard in adopting the fourth axiom of the set

$$(e^{\lambda})^{\theta} = e^{\lambda\theta}, \tag{1}$$
$$(e^{i\lambda})^{\theta} = e^{i\lambda\theta}, \tag{2}$$
$$(e^{\lambda})^{i\theta} = e^{i\lambda\theta}, \tag{3}$$
$$(e^{i\lambda})^{i\theta} = e^{i\lambda\theta}. \tag{4}$$

$\square\leftarrow$

For example (consistently!)

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

and

$$\begin{aligned}(1^i)^0 = (1^0)^i = 1^i &= (i.i.i.i)^i \\ &= i^i.i^i.i^i.i^i \\ &= i.i.i.i \\ &= 1. \square\end{aligned}$$

For x = a + bi, under the $\mathbb{D}1$ algebra

$$(a + bi)^{c + di} = (a + bi)^c(a + bi)^{di},$$

which in polar coordinates is of the form

$$[r^c e^{i\theta c}][r^{di}e^{i\theta d}] = r^{c + di}[\cos\theta(c + d) + i\sin\theta(c + d)]$$
$$= e^{fc}[\cos fd + i\sin fd][\cos\theta(c + d) + i\sin\theta(c + d)]. \square \tag{5}$$

We now see why there may be an obstruction to an extension of the reciprocity theorems to congruence arithmetic in powers for Gaussian integers. For a natural number n > 1, the expansion in the $\mathbb{D}1$ algebra of

$$\begin{aligned}n^i &\equiv (1 + (n - 1))^i \pmod u \\ &\equiv 1 + i(n - 1) + [i(i - 1)/2](n - 1)^2 + [i(i - 1)(i - 2)/3!](n - 1)^3 + \ldots \pmod u,\end{aligned} \tag{6}$$

which is an infinite series, contains terms with u in the denominator, and this is equivalent to dividing by zero. Thus we evaluate (6) in characteristic zero and only subsequently impose the condition (mod u). Nevertheless, if the series is transcendental, totient theorems as usually conceived do not apply, although we may employ an exponential congruence arithmetic.

There is a way around obstructions of this type if we observe that in algebra $\mathbb{D}1$ the expression $e^{r\pi/k + in\pi/m}$, when raised to the power i becomes $e^{ir\pi/k + in\pi/m}$, and we can now determine these expressions (mod $e^{i\theta}$) for some suitable θ, and also multiplying natural numbers or their rational or complex number congruence equivalents by expressions of this form. $\square$

The lower intricate $\mathbb{D}1$ algebra is also detailed in [Ad14]. We designate as the equivalent of equations (1) – (4), when θ and λ are real and the matrix J may not equal J′ but 10.(3) holds for J and J′, that the following spectrum of algebraic equations hold

$(e^{\lambda})^{\theta} = e^{\lambda\theta}$, (7)

$(e^{\lambda J})^{\theta} = e^{J\lambda\theta}$, (8)

$(e^{\lambda})^{J'\theta} = e^{J'\lambda\theta}$, (9)

$(e^{J\lambda})^{J'\theta} = e^{J\lambda\theta}$. (10)

The J and J′ are held fixed at each exponential level of nested brackets above. It is not the case that the same evaluations pertain for different values of J and J′, but a choice once made is consistent.

We will evaluate $(e^{\rho+J\lambda})^{J'\theta}$ as $e^{\rho\theta J'}e^{\lambda\theta J}$, noting that this is not $e^{\rho\theta J'+\lambda\theta J}$ when $J \neq J'$. The above configuration cannot accommodate intricate numbers with negative determinant. For that, we designate such numbers by $e^{\sigma} + e^{\rho+\theta J}$. The change of basis of $bi + c\alpha + d\phi$ is called a ***JAF*** transformation. The restrictive 'J-abelian' criterion for hyperintricate numbers makes them more amenable to calculation. These aspects are more fully described in [Ad14]. □

References.

I have transcribed the text of [Ma1886] almost verbatim where it occurs, on the grounds that the best exposition from this author is arrived at by allowing him to speak entirely for himself.

The Fundamenta nova and gesammelte Werke of Jacobi, which are recommended (the former is contained in the latter), may be viewed in the UK at the British library, but are not available on inter-library loans from it. I have therefore inserted the suggestion [Ca1895].

I have made a translation from the French of [Ei1845] taken from Eisenstein's Mathematiche Abhandlungen, which is available on request from the author at jim-adams@supanet.com. There is a commentary on this work by Kronecker, both in German [Kr1876] and French [Kr1880].

Ad11	J.H. Adams, *An elementary investigation of the prime* p = 4k – 1 *asymmetry theorem for quadratic residues* I, 2011.
Ad13	J.H. Adams, *Discussion on ladder numbers and zero algebras*, 2013.
Ad14	J.H. Adams, *Superexponential algebra*, 2014.
Ca1895	A. Cayley, *An elementary treatise on elliptic functions*, 1895, reprinted Dover 1961.
CG00	J.H. Conway and R.K. Guy, *The book of numbers*, Copernicus books, Springer, 2000.
Ei1845	G. Eisenstein, *2. Applications de l'Algèbra à l'Arithmétique transcendante*, 1845, Mathematische Abhandlungen, Georg Olms Hildesheim, 1967.
Eu300BC	Euclid, *The thirteen books of the elements*, tr T.L. Heath.
Ga1846	É. Galois, *Oeuvres mathematiques*, Journal des mathématiques pures et appliquées **XI**: 381–444.
Ga62	É. Galois, *Écrits et mémoires mathématiques*, Gautier Villars (pp 539), 1962.
Ja1829	C.G. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, 1829.
Kr1876	L. Kronecker, II. *Ueber das Reciprocitätsgesetz*, 1876, vol. 2, Werke, ed. K. Hensel, reprinted Chelsea Publishing, 1968.
Kr1880	L. Kronecker, III. *Sur la loi de réciprocité*, 1880, vol. 2, Werke.
Ma1886	G.B. Mathews, *Theory of Numbers*, 1886, reprinted Chelsea Publishing.
1We76	A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Springer, 1976.
2We40	H. Weyl, *Algebraic theory of numbers*, Princeton U. P., 1940.