

PROVING QUADRATIC RECIPROCITY

Andrew Boucher

Created: 9 June 2003

12 November 2003

Version 1.1

www.andrewboucher.com/papers/quadratic_reciprocity.pdf

A. General Introduction

These notes are meant to continue from the paper on Consistency, in proving number-theoretic theorems from the second-order arithmetical system called **F**. Its ultimate target is Quadratic Reciprocity, although it introduces and proves some facts about the least common multiple at the start.

An attempt has been made to keep this paper as self-contained as possible. Nonetheless, prior knowledge of and familiarity with the Consistency paper (to be found at www.andrewboucher.com/papers/consistency.pdf) would make comprehension easier.

F works in second-order logic with equality (equality is not defined and axioms of equality are assumed). It assumes arithmetic aka predicative comprehension and the following axioms:

(F1) Uniqueness of numbering.

$\forall n \forall m \forall P (Nn \ \& \ Mn,P \ \& \ Mm,P \ \Rightarrow \ n = m)$

(F2) Zero.

$\forall P (M0,P \Leftrightarrow \neg \exists x Px)$

(F3) Successoring.

$\forall n \forall m \forall P \forall Q \forall a (Nn \ \& \ \sigma_{n,m} \ \& \ \neg Pa \ \& \ \forall x (Qx \Leftrightarrow Px \vee x = a) \Rightarrow (Mn,P \Leftrightarrow Mm,Q)$
)

(F4) Induction. Let ϕ be a well-formed formula (with no appearance of m). Use $\phi[x \setminus y]$ to mean x replaces all (free) instances of y . Suppose $\phi[0 \setminus n]$ and $\forall n \forall m (Nn \ \& \ \sigma_{n,m} \ \& \ \phi \Rightarrow \phi[m \setminus n])$. Then $\forall n (Nn \Rightarrow \phi)$

F has as models: the standard model and any initial segment, including the

singleton model $\{0\}$. It turns out it can prove, given any natural number n , that all numbers less than n exists. But it cannot prove that any number greater than n exists, because it does not assume the *ad infinitum* axiom, namely

$$\forall n \forall P \forall a (Nn \ \& \ Mn,P \ \& \ \neg Pa \Rightarrow \exists m (Nm \ \& \ Mm,(P \cup \{a\}))).$$

In the Consistency paper it is shown that **F** can prove much of elementary arithmetic, including the Euclidean Algorithm and Unique Prime Factorization.

F cannot prove Commutativity of Addition written as

$$\forall n \forall m (n + m = m + n)$$

but can in the form

$$\forall n \forall m \forall k (n + m = k \Rightarrow m + n = k).$$

It is perhaps instructive to comment on the difference between the two versions. The first asserts not only Commutativity, but also that $n + m$ and $m + n$ exist; for if they didn't exist, they couldn't be equal. But **F** cannot prove that bigger numbers exist given the existence of smaller ones, so it cannot establish this version. The second one, however, *assumes*, the existence of $n + m$, by supposing $n + m = k$. Given this assumption, it can then establish that $m + n$ exists and indeed equals k .

Quadratic Reciprocity is chosen as the ultimate aim of this paper because of its historical importance. Also, the proof which the author first learned, which is also the one in Hardy and Wright's *An Introduction to the Theory of Numbers*, makes essential use of the *ad infinitum* principle. That is, Quadratic Reciprocity makes an assertion about when two odd prime numbers p and q both have another number as a quadratic residue. The proof in Hardy and Wright is a counting argument - one counts the points in a rectangular grid which is $(p-1)/2$ points long and $(q-1)/2$ points high. Of course, such number of points is greater than either p or q , so the *ad*

infinitum principle must be invoked to establish that all these points *have* a number.

In fact, as we shall see, the counting argument can be replaced by a consideration of parity alone, which thus avoids an appeal to *ad infinitum*.

The knowledgeable reader will find the pace slow. In order not to burden the proceedings too much at the outset, subtraction, which was not introduced in *Consistency*, will be assumed here. That is, if $(x+y) = z$, then we may use $(z-y)$ to refer to the (unique) x . We will also assume any basic law concerning subtraction (e.g. distribution with respect to multiplication). Remark that, since we are working only in the natural numbers, if $(z-y)$ is asserted (positively) of something, then we may infer that $z \geq y$.

Certain liberties will also be taken. For instance *Consistency* uses a predicate *one* in order to speak of something being the number one, rather than a constant symbol 1, because the latter presupposes its existence. Nonetheless, this paper falls into the latter habit, in order to avoid verbosity. The reader may check that 1 is only used when its existence is being assumed; or, if its existence is being asserted, only when such existence follows from the assumptions. (Similarly for 2 and other numbers.)

Sequences in *Consistency* began with 1, i.e. if $Seq(R,n)$, then R is a sequence of length n , namely $(R'1), (R'2), \dots, (R'n)$. This paper will use smaller-case letters and subscripts to better conform with mathematical usage. Also, introduce the notion of a sequence beginning with 0 and ending in n :

A.1 *Def.* $Seq0(R,n)$ if and only if R is a function relation with domain $[0 _ n]$, for some $n \geq 0$.

Propositions in *Consistency* will be referred to with a “II” prefixed. So II.N.4 refers to N.4 in that paper. When “II” is not prefixed, the reference is a proposition in the present paper.

Lastly, I should acknowledge having followed David Burton's *Elementary Number Theory* and Hardy & Wright.

B. The Least Common Multiple

Results of this section are *not* used subsequently in the present paper, so it may be skipped.

B.1 Prop. Suppose $x|z$, $y|z$, and $\text{one}(x \Delta y)$. Then $x^*y|z$.

Remark: $(x \Delta y)$ is our idiosyncratic way to write “the greatest common divisor of x and y .” It was introduced in *The Foundations of Elementary Arithmetic*, where a *defieniens* needed to be a single symbol (thereby ruling out the use of “gcd”).

Pf:

Consider the unique prime factorization of z , by II.N.4. Part of the factorization must be that of x , and (since x and y are relatively prime) a different part must be that of y . But then $x^*y|z$. \square

B.2 Prop. Suppose $(x \Delta z) = 1$ & $(y \Delta z) = 1$ and that x^*y exists. Then $(x^*y \Delta z) = 1$.

Pf:

Suppose $c|x^*y$ & $c|z$, with $c \geq 2$. WLOG we may suppose $\pi(c)$, i.e. c is a prime. Then by II.N.3 $c|x$ or $c|y$. But this contradicts $(x \Delta z) = 1$ & $(y \Delta z) = 1$. \square

B.3 Prop. Suppose $(x \Delta y) = 1$, and suppose Nd & $\neg d = 0$. Then there exist e, f s.t. $(e \Delta x) = 1$ & $(f \Delta y) = 1$ & $(e \Delta f) = 1$ & $e^*f = d$.

Pf:

Consider the unique prime factorization of d , by II.N.4. Since $(x \Delta y) = 1$, they have no common prime factors. So evidently there exist e, f s.t. e has none of the prime factors of x , f has none of the prime factors of y , e and f share no common prime factors, and $e^*f = d$.

The next lemma uses traditional notation where sequences are smaller case letters and values of sequences are letters with subscripts.

B.4 *Lemma.* Suppose

$$\begin{aligned} & \text{Seq}(q,c) \ \& \ \text{Seq}(r,c+2) \ \& \\ & r_1 = a \ \& \ r_2 = b \ \& \ r_{c+1} = (a \ \Delta \ b) \ \& \ r_{c+2} = 0 \ \& \\ & \ \& \ \forall i \ (0 < c \leq i \Rightarrow r_i = q_i * r_{i+1} + r_{i+2} \ \& \ r_{i+2} < r_{i+1}), \end{aligned}$$

i.e. the conditions of the Euclidean Algorithm apply. Then, for all i with $2 \leq i \leq c$, if $(r_{i-1} * r_i)$ exists, then $\exists u, v$ s.t. $u \leq r_{i-1}$ & $v \leq r_i$ and either

$$\begin{aligned} (a \ \Delta \ b) &= (u * r_i - v * r_{i-1}) \ \text{or} \\ (a \ \Delta \ b) &= (v * r_{i-1} - u * r_i). \end{aligned}$$

Pf.

Proceed by induction, downward on i , i.e. the base step is $i = c$, and in the induction step, we decrease i by 1.

Now

$$r_{c-1} = q_{c-1} * r_c + r_{c+1}.$$

$r_{c+1} < r_c$, so $1 \leq r_c$. Also $q_{c-1} \leq r_{c-1}$. But

$$(a \ \Delta \ b) = r_{c+1} = 1 * r_{c-1} - q_{c-1} * r_c$$

So the assertion is true for $i = c$.

Now suppose it is true for $i = k > 2$. We will show it is true for $(k-1)$.

So suppose $r_{k-2} * r_{k-1}$ exists. By monotonicity, $r_{k-1} * r_k$ exists. By the inductive assumption,

$$(a \ \Delta \ b) = u * r_k - v * r_{k-1}$$

or

$$(a \ \Delta \ b) = v * r_{k-1} - u * r_k,$$

for some u, v , where $u \leq r_{k-1}$ and $v \leq r_k$. Assume the first (the proof of the second case is similar). Use

$$r_{k-2} = q_{k-2} * r_{k-1} + r_k,$$

and substitute to get

$$(a \ \Delta \ b) = u * (r_{k-2} - q_{k-2} * r_{k-1}) - v * r_{k-1}$$

$u \leq r_{k-1}$, so $(u * r_{k-2}) \leq (r_{k-1} * r_{k-2})$, which exists by supposition. The

other numbers are evidently less, so distributivity applies, and the equation can be manipulated into

$$c = u * r_{k-2} - (u * q_{k-2} + v) * r_{k-1}$$

Finally, note that

$$u * q_k + v \leq q_k * r_{k-1} + r_k.$$

□

B.5 Prop. Suppose (a^*b) exists, with either a or b non-zero. Then $\exists u, v$ s.t.

$$(a \Delta b) = u^*a - v^*b \text{ or}$$

$$(a \Delta b) = v^*b - u^*a.$$

Remark: the assumption that (a^*b) exists will be improved on in a subsequent proposition.

Pf:

Obvious if $a, b \leq 2$.

Otherwise, we may suppose either a or $b > 2$, and so that \exists exists.

The Euclidean Algorithm K.2 therefore applies. By the previous

lemma,

$$(a \Delta b) = u^*a - v^*b \text{ or}$$

$$(a \Delta b) = v^*b - u^*a,$$

for some u, v . □

B.6 Def. Let N_x & N_y . We say that z is the *least common multiple* of x and y if both:

$$\text{i) } x | z \text{ and } y | z$$

$$\text{ii) if } x | k \text{ and } y | k, \text{ then } z \leq k$$

We write z (obviously unique) as $(x \diamond y)$.

Unlike the greatest common divisor, it is not assured, given two numbers, that their least common multiple exists, since this would usually be a bigger number. However, since $(x * y)$ is evidently a common multiple of x and y , if this exists, then the least common multiple does as well.

B.7 Prop

$$1) \forall x \forall y \forall z ((x \diamond y) = z \Rightarrow (y \diamond x) = z)$$

$$2) \forall x \forall y \forall z ((x \diamond y) = z \Rightarrow x | z)$$

$$3) \forall x \forall y \forall z ((x \diamond y) = z \Rightarrow x \leq z)$$

- 4) $\forall x \forall y \forall z ((x \diamond y) = z \ \& \ x | y \Rightarrow z = y)$
 5) $\forall x (Nx \Rightarrow (x \diamond 0) = 0)$
 6) $\forall x (Nx \ \& \ \text{one}(1) \Rightarrow (x \diamond 1) = x)$

B.8 Prop. Suppose $(x * y)$ exists, and one of x and y is not zero. Then:

- 1) $(x \Delta y) * (x \diamond y) = x * y$.
 2) $(x \diamond y) = (x \Delta y) * x' * y'$, for some x', y' s.t. $x = (x \Delta y) * x'$ and $y = (x \Delta y) * y'$.

Pf.

Let $d = (x \Delta y)$, which exists since one of x and y is not zero. Set $c = (x \diamond y)$, which exists since $(x * y)$ does. By II.H.5.2, $x = d * x'$ and $y = d * y'$ for some natural numbers x', y' . By II.H.5.11 $(x' \Delta y') = 1$. By B.3 there exist e, f such that $(e \Delta x') = 1 \ \& \ (f \Delta y') = 1 \ \& \ (e \Delta f) = 1 \ \& \ e * f = d$. By B.2 $(x' * f \Delta y') = 1$ and $(x' * f \Delta e) = 1$, so $(x' * f \Delta y' * e) = 1$. Since $x' * f | c$ and $y' * e | c$, then by B.1 $x' * e * y' * f | c$. Rearranging, $x * y' | c$. On the other hand, $x * y'$ is a common multiple of x and y , so $c \leq x * y'$. Thus $x * y' = c$, and so $d * c = d * (x * y') = x * y$. \square

B.9 Proposition. Suppose $(a \diamond b)$ exists, with either a or b non-zero, and where $s * a = t * b = (a \diamond b)$ for some s, t . Then $\exists u, v$ such that $u \leq s, v \leq t$, and

$$(a \Delta b) = u * a - v * b$$

or

$$(a \Delta b) = v * b - u * a.$$

Proof.

Let $d = (a \Delta b)$, which exists since both x and y are not zero. By B.8.2 $(a \diamond b) = d * a' * b'$, for some a', b' s.t. $a = (a \Delta b) * a'$ and $b = (a \Delta b) * b'$. Evidently $(a' * b')$ exists, so by ?? $\exists u, v$ s.t. $u \leq b' \ \& \ v \leq a'$ and

$$(a' \Delta b') = u * a' - v * b' \ \text{or}$$

$$(a' \Delta b') = v * b' - u * a'.$$

Consider the first case (the proof of the second is similar). Now by H.5.11

$(a' \Delta b') = 1$, so

$$1 = u * a' - v * b'.$$

So

$$d = d * (u * a' - v * b').$$

Since $u \leq b'$ and $d * a' * b'$ evidently exists, so does $d * u * a'$. Similarly, $d * v * b'$ exists, so distribution applies, and

$$d = d * u * a' - d * v * b'$$

Rearranging

$$d = u * (d*a') - v * (d*b'), \text{ i.e.}$$

$$d = u * a - v * b.$$

By construction $b' = s$ and $a' = t$.

□

B.10 *Prop.* Suppose $(a \diamond b)$ exists, with either a or b non-zero. Then:

$$1) \exists u \leq s, v \leq t \text{ s.t. } (a \Delta b) = u*a - v*b$$

and

$$2) \exists u \leq s, v \leq t \text{ s.t. } (a \Delta b) = v*b - u*a.$$

Proof:

By B.9 either 1) or 2) holds. We will show that, if 1) holds, then 2) does as well.

For suppose

$$(a \Delta b) = u*a - v*b$$

for some $u \leq s, v \leq t$ where $s*a = t*b = (a \diamond b)$. Then

$$\begin{aligned} (a \Delta b) &= (u*a - v*b) + (t*b - s*a) \\ &= (t - v) * b - (s - u) * a \end{aligned}$$

Evidently $t - v \leq t$ and $s - u \leq s$. □

C. Congruences

C.1 *Def.* Let $n > 0, Na$. Use $rm(a,n)$ to denote the unique number which is the remainder term guaranteed by division, i.e. $rm(a,n) = r$ where

$$a = n*q + r \text{ and } 0 \leq r < n \text{ for some } q \text{ with } Nq.$$

C.2 *Def.* Let $n > 0$. Write

$$a \equiv_n b$$

or

$$a \equiv b \pmod{n}$$

when $rm(a,n) = rm(b,n)$. We say a is *congruent to* $b \pmod{n}$. When n (called the *modulus*) can be understood, it may be omitted, leaving $a \equiv b$ or the like.

Remark: “ \equiv ” has already been used to express predicate equivalence. Since both sides are big letters in that case, and small letters here, there should

be no confusion.

The next two propositions are obvious. Remark that, by our usual convention, if $a \equiv b \pmod{n}$, then we can infer that Na, Nb, Nn , and $n > 0$.

C.3 Prop. \equiv is an equivalence relation. I.e. let $n > 0, Na$. Then:

- 1) $a \equiv a \pmod{n}$
- 2) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
- 3) $a \equiv b \pmod{n} \ \& \ b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

C.4 Prop. Let $n > 0$.

- 1) If $(k * n)$ exists, then $(k * n) \equiv 0 \pmod{n}$
- 2) If $a \equiv 0 \pmod{n}$, then $a = (k * n)$ for some k .
- 3) $a \equiv 0 \pmod{n} \Leftrightarrow n \mid a$
- 4) $a \equiv b \pmod{n} \ \& \ a, b < n \Rightarrow a = b$
- 5) $a \equiv b \pmod{n} \Rightarrow n \mid (b - a) \vee n \mid (a - b)$. (Indeed which disjunct holds depends on whether $b \leq a$ or $a \leq b$, respectively.)

D. Congruence Addition

D.1 Def. Let $n > 0, Na, Nb$, and set $a' = rm(a,n)$, $b' = rm(b,n)$. Then use $(a \oplus_n b)$ to denote:

$$\begin{cases} a \oplus_n b & \text{if } a \oplus_n b < n \\ b \oplus_n (n - a) & \text{otherwise} \end{cases}$$

The subscripted n (called the *modulus*) may be omitted if capable of being understood.

Remark: Note that $b' - (n - a')$ is defined in the second case. For $rm(a,n) < n$. And were $(n - a') > b'$, then $n > (a' + b')$, contrary to the assumption governing the second case.

D.2. Prop. Let $n > 0$ be the modulus.

- 1) $Na \ \& \ Nb \Rightarrow 0 \leq a \oplus b < n$
- 2) $a < n \ \& \ b < n \Rightarrow (a \oplus b = 0 \Leftrightarrow (a = 0 \ \& \ b = 0) \vee (a + b = n))$
- 3) $a \oplus b \equiv c \oplus d \Rightarrow a \oplus b = c \oplus d$

- 4) $a \equiv c \ \& \ b \equiv d \Rightarrow a \oplus b = c \oplus d$
- 5) $a + b = c \Rightarrow a \oplus b \equiv c$
- 6) $a + b = c \ \& \ c < n \Rightarrow a \oplus b = c$
- 7) $Na \ \& \ Nb \Rightarrow a \oplus b \equiv b \oplus a$
- 8) $Na \ \& \ Nb \ \& \ Nc \Rightarrow a \oplus (b \oplus c) \equiv (a \oplus b) \oplus c$
- 9) $Na \Rightarrow a \oplus 0 \equiv a$
- 10) $a \oplus b \equiv a \oplus c \Rightarrow b \equiv c$

Pf:

5) Let $a = q_a * n + r_a$, $b = q_b * n + r_b$, where $0 \leq r_a, r_b < n$. Then

$$c = (q_a + q_b) * n + (r_a + r_b).$$

If $(r_a + r_b) < n$, then $a \oplus b = r_a + r_b = rm(c, n)$. Since of course then $rm(a \oplus b, n) = (r_a + r_b)$ as well, $(a \oplus b) \equiv c$. On the other hand, if $(r_a + r_b) \geq n$, then $rm(c, n) = (r_a + r_b) - n = r_b - (n - r_a)$, so again $(a \oplus b) \equiv c$.

8) By cases.

10) By cases.

□

D.3 *Prop.* Suppose $d \mid n$, and that

$$a \equiv 0 \pmod{n}$$

$$b \equiv 0 \pmod{n}.$$

Then

$$a \oplus_n b \equiv 0 \pmod{d}.$$

Pf:

By C.4.3 $d \mid a$ and $d \mid b$. By the Division Algorithm II.G.3, there exist s, t, a', b' such that

$$a = n*s + a' \text{ with } 0 \leq a' < n$$

$$b = n*t + b' \text{ with } 0 \leq b' < n$$

Clearly $d \mid a'$ and $d \mid b'$. So $d \mid (a' + b')$ if $(a' + b')$ exists, and otherwise $d \mid (b' - (n - a'))$. But then $d \mid (a \oplus_n b)$. □

D.4 *Prop.* Let $n > 0$ be the modulus.

1) $Na \Rightarrow \exists c (a \oplus c) = 0$. Moreover, there is only one such $c < n$.

2) $Na \ \& \ b < n \Rightarrow \exists c (a \oplus c) = b$. Moreover, there is only one such $c < n$.

Pf:

1) If $a = 0$, use $c = 0$. Otherwise use $c = n - rm(a,n)$. Uniqueness follows by D.2.10 and C.4.4. \square

Indeed,

D.5 *Prop.* Let $n > 0$ be the modulus. Then:
 $a \oplus c = 0$ & $0 < c \leq n \Rightarrow c = n - rm(a,n)$.

D.6 *Def.* Let $n > 0$, $Seq(r,m)$, and $k \leq m$. Use $(n \sum_1^k r_i)$ to refer to the (evidently unique) y , if it exists, such that

$$\exists s (Seq0(s,k) \ \& \ s_0 = 0 \ \& \ s_k = y \ \& \ \forall j (j < k \Rightarrow s_{j+1} = s_j \oplus_n r_{j+1})).$$

Clearly, $(n \sum_1^0 r_i) = 0$ for any sequence r , when $n > 0$.

We shall abuse the notation as needed. In particular, when the modulus n can be understood, it will be dropped.

E. Congruence Multiplication

E.1 *Def.* Let $n \geq 1$, Na , Nb . Set $(a \otimes_n b)$ to

$$n \sum_1^a r_i,$$

where $r_i = b$ for all i , $1 \leq i \leq a$.

Note: As usual, the n subscript may be dropped if it can be understood.

E.2 *Prop.* Let $n \geq 1$, Na , Nb . Then $(a \otimes_n b)$ exists. Also, if $(a+1)$ exists, then
 $(a+1) \otimes_n b = (a \otimes_n b) \oplus_n b$.

E.3 *Prop.* Let $n \geq 1$ be the modulus.

- 1) $Na \ \& \ Nb \Rightarrow 0 \leq a \otimes b < n$
- 2) $a \otimes b \equiv c \otimes d \Rightarrow a \otimes b = c \otimes d$
- 3) $Na \Rightarrow 0 \otimes a = 0$
- 4) $a \equiv 0 \Rightarrow b \otimes a = 0$
- 5) $Na \Rightarrow 1 \otimes a \equiv a.$
- 6) $Na \ \& \ b \equiv b' \Rightarrow a \otimes b = a \otimes b'$
- 7) $Na \ \& \ Nb \Rightarrow a \otimes (b \oplus 1) = (a \otimes b) \oplus a$
- 8) $a \equiv 0 \Rightarrow a \otimes b = 0$
- 9) $Na \ \& \ Nb \Rightarrow a \otimes b = b \otimes a$
- 10) $Na \ \& \ Nb \ \& \ Nc \Rightarrow a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
- 11) $Na \ \& \ Nb \ \& \ Nc \Rightarrow a \otimes (b \otimes c) = (a \otimes b) \otimes c$
- 12) $a * b = c \Rightarrow a \otimes b \equiv c$
- 13) $x \leq n \ \& \ y \leq n \Rightarrow (n - x) \otimes (n - y) = x \otimes y$
- 14) $x \otimes y > 0 \Rightarrow (n - x) \otimes y = n - (x \otimes y)$
- 15) $(x \otimes y) = 0 \Rightarrow (n - x) \otimes y = 0$

Pf:

3) $n \sum_i^0 r_i = 0$ for any sequence r .

4) By induction on b . $(0 \otimes a) = 0$ by 3). Now suppose $a \equiv 0$ and $(b \otimes a) = 0$. By E.2

$$(b+1) \otimes a = (b \otimes a) \oplus a = 0 \oplus a \equiv a \equiv 0.$$

By 1) and C.4.4 $(b+1) \otimes a = 0$.

5) $1 \otimes a = (0 \otimes a) \oplus a$ by E.2
 $= (0 \oplus a) \equiv a$ by 3) and D.2.9

6) By induction on a .

$$0 \otimes b = 0 = 0 \otimes b' \text{ by 3),}$$

so true when $a = 0$.

$$\text{Now suppose } Na \ \& \ b \equiv b' \ \& \ a \otimes b = a \otimes b'.$$

By E.2

$$(a + 1) \otimes b \equiv (a \otimes b) \oplus b \text{ and}$$

$$(a + 1) \otimes b' \equiv (a \otimes b') \oplus b'.$$

The result follows from the induction hypothesis and D.2.4.

7) By induction on a .

$$0 \otimes (b \oplus 1) = 0 = 0 \oplus 0 = (0 \otimes b) \oplus 0,$$

so true when $a = 0$.

Now suppose Na & Nb & $a \otimes (b \oplus 1) = (a \otimes b) \oplus a$.

Then

$$\begin{aligned}
 (a + 1) \otimes (b \oplus 1) &= a \otimes (b \oplus 1) \oplus (b \oplus 1) \text{ by E.2} \\
 &= ((a \otimes b) \oplus a) \oplus (b \oplus 1) \text{ by the inductive hypothesis} \\
 &= ((a \otimes b) \oplus b) \oplus (a \oplus 1) \text{ by Commutativity and Associativity} \\
 &= ((a + 1) \otimes b) \oplus (a \oplus 1) \text{ by E.2} \\
 &= ((a + 1) \otimes b) \oplus (a + 1) \text{ D.2.5 and D.2.4}
 \end{aligned}$$

8) By induction on b . $b = 0 \Rightarrow a \otimes b = 0$ by 3). For the induction step, suppose $a = 0$ and $a \otimes b = 0$. Then

$$\begin{aligned}
 a \otimes (b + 1) &= a \otimes (b \oplus 1) \text{ by D.2.5 and 6)} \\
 &= (a \otimes b) \oplus a \text{ by 7)} \\
 &= 0 \oplus 0 \text{ by D.2.4} \\
 &= 0 \text{ by D.2.2.}
 \end{aligned}$$

9) By induction on a . $0 \otimes b = 0 = b \otimes 0$ by 3) and 4).

For the induction step, suppose Na & Nb & $a \otimes b = b \otimes a$. Then

$$\begin{aligned}
 (a + 1) \otimes b &= (a \otimes b) \oplus b \text{ by E.2} \\
 &= (b \otimes a) \oplus b \text{ by the induction hypothesis} \\
 &= b \otimes (a \oplus 1) \text{ by 7)} \\
 &= b \otimes (a + 1) \text{ D.2.5 and D.2.4}
 \end{aligned}$$

10) By induction on a .

11) By induction on a .

13) Let $x \leq n$ & $y \leq n$. By D.4.1 it suffices to note that both $x \otimes y$ and $(n - x) \otimes (n - y)$ are the additive inverses of $x \otimes (n - y)$.

□

E.4 *Prop.* Let Na & Nx & $n \geq 1$. Then $(a \Delta n) \mid (a \otimes_n x)$.

Pf:

By induction on x . If $x = 0$, then $a \otimes_n x = 0$, and the result follows.

Now suppose $(a \Delta n) \mid (a \otimes_n x)$. Then by E.3.9 and E.2

$$a \otimes_n (x+1) = (x \otimes_n a) \oplus_n a.$$

The result follows by another application of E.3.9, the induction hypothesis, and D.3.

□

Note: Obviously, also $(x \Delta n) \mid (a \otimes_n x)$.

E.5 *Prop.* $(c \Delta n) = 1 \ \& \ c \otimes_n a = 0 \Rightarrow a \equiv 0 \pmod{n}$.

Pf.

Suppose c is the smallest x such that

$$(x \Delta n) = 1 \ \& \ x \otimes_n a = 0 \ \& \ \neg a \equiv 0 \pmod{n}.$$

Hence

$$(c \Delta n) = 1 \ \& \ c \otimes_n a = 0 \ \& \ \neg a \equiv 0 \pmod{n}.$$

If $c = 0$, then $n = 1$ since $(c \Delta n) = 1$. But $a \equiv 0 \pmod{1}$ for all a , contradicting the last conjunct.

So $c > 0$. Hence there are q, r such that

$$n = q * c + r, \text{ where } 0 \leq r < c.$$

By D.2.5 and E.3.12,

$$n \equiv q \otimes c \oplus r.$$

So

$$0 \equiv q \otimes c \oplus r$$

$$0 \otimes a \equiv (q \otimes c \oplus r) \otimes a \quad \text{by E.3.6}$$

$$0 \equiv (q \otimes c \oplus r) \otimes a \quad \text{by E.3.3}$$

$$0 \equiv (q \otimes c \otimes a) \oplus (r \otimes a) \quad \text{by E.3.10}$$

$$0 \equiv (q \otimes 0) \oplus (r \otimes a) \quad \text{by assumption}$$

$$0 \equiv 0 \oplus (r \otimes a) \quad \text{by E.3.4}$$

$$0 \equiv (r \otimes a) \quad \text{by D.2.9}$$

But

$$(r \Delta n) = (c \Delta n) = 1.$$

Since $r < c$, this is a contradiction.

□

Remark: The previous proposition provides another way to prove II.N.1 and II.N.5 (Euclid's Lemma).

E.6 *Corollary.* Suppose $(c \Delta n) = 1 \ \& \ c \otimes_n a = c \otimes_n b$. Then $a \equiv b \pmod{n}$.

E.7 *Prop.* Suppose $(c \Delta n) = 1$. Then

$$0 \otimes_n c, 1 \otimes_n c, \dots, (n-1) \otimes_n c$$

are the numbers $0, 1, \dots, (n-1)$, perhaps in a different order.

Pf.

It suffices to establish that the list has no repetitions. For, if they are

distinct, then there are n entries. But by E.3.1, they are all within 0 and $n-1$, and there are of course n of these. By II.E.10 the two lists would contain the same numbers.

So, suppose $i \otimes_n c = j \otimes_n c$. By the corollary E.6 $j = i$. By C.4.4, $j = i$ since both are $< n$.

□

E.8 *Corollary.* Suppose $(c \Delta n) = 1$. Then

$$1 \otimes_n c, 2 \otimes_n c, \dots, (n-1) \otimes_n c$$

are the numbers $1, 2, \dots, (n-1)$, perhaps in a different order.

E.9 *Corollary.* Suppose $(c \Delta n) = 1$, and $0 \leq b < n-1$. Then

$$c \otimes_n x = b$$

has a unique solution (for x) among $0, 1, \dots, (n-1)$. Any other solution is congruent to this solution.

E.10 *Prop.* $c \otimes_n x = b$ has a solution if and only if $0 \leq b < n$ and $(c \Delta n) \mid b$.

Pf:

$$(\Rightarrow) \text{ Suppose } (c \otimes_n x) = b. \text{ By E.4, } (c \Delta n) \mid (c \otimes_n x) = b.$$

(\Leftarrow) Suppose $0 \leq b < n$ and $(c \Delta n) \mid b$. Set $d = (c \Delta n)$. Then there exist b', a' such that $b = (b' * d)$ and $c = (c' * d)$. So $(c' \Delta n) = 1$ and hence by E.7

$(c' \otimes_n x) = b'$ for some x . Thus $d \otimes_n c' \otimes_n x = d \otimes_n b' = b$, hence by E.3.12 and E.3.6, $(c \otimes_n x) = b$.

□

E.11 *Prop.* Let $n \geq 1$, Na, Nb . Suppose $\neg (b \Delta n) = 1$. Then

$$\neg (a \otimes_n b \Delta n) = 1. \text{ Indeed, } (b \Delta n) \mid (a \otimes_n b \Delta n).$$

Pf:

$$\text{By E.4, } (b \Delta n) \mid (a \otimes_n b). \text{ Since } (b \Delta n) \mid n \text{ as well, by II.H.5.10}$$

$$(b \Delta n) \mid (a \otimes_n b \Delta n). \quad \square$$

E.12 *Prop.* Let $n \geq 1$. Suppose $(a \Delta n) = (b \Delta n) = 1$. Then $(a \otimes_n b \Delta n) = 1$.

Pf.

By E.9 there exists c such that $(c \otimes_n a) = 1$.

Suppose $\neg (a \otimes_n b \Delta n) = 1$. By E.11 $\neg (c \otimes_n a \otimes_n b \Delta n) = 1$. Now $c \otimes_n a \otimes_n b = 1 \otimes_n b = \text{rm}(b,n)$, so $\neg (\text{rm}(b,n) \Delta n) = 1$. $\neg (b' \Delta n) = 1$, where $b' = \text{rm}(b,n)$. But $(b \Delta n) = (b' \Delta n)$ by II.H.5.7, contradicting $(b \Delta n) = 1$. Whence, $((a \otimes_n b) \Delta n) = 1$. \square

E.13 *Def.* Let $n > 0$, $\text{Seq}(R,n)$, and $k \leq n$. Use $(n \prod_1^k r_i)$ to refer to the (evidently unique) y , if it exists, such that

$$\begin{aligned} \exists s (\text{Seq}0(s,k) \ \& \ s_0 = 1 \ \& \ s_k = y \ \& \\ \forall j (j < k \Rightarrow s_{j+1} = s_j \otimes_n r_{j+1})). \end{aligned}$$

Clearly $(n \prod_1^0 r_i) = 1$, when $n > 0$.

F. Congruence Exponentiation

F.1 *Def.* Let $n \geq 1$, Na , Nb . Set $(b \Theta_n a)$ to

$$n \prod_1^a r_i,$$

where $r_i = b$ for all i , $1 \leq i \leq a$.

Note: As usual, the n subscript may be dropped if it can be understood.

F.2 *Prop.* Let $n \geq 1$, Na , Nb . Then:

- 1) $b \Theta_n a$ exists.
- 2) $b \Theta_n 0 = 1$. (*Note:* this includes $b = 0$, so $0 \Theta_n 0 = 1$.)
- 3) $b \Theta_n 1 = b$.
- 4) If $a+1 \geq 1$, then $b \Theta_n (a+1) = (b \Theta_n a) \otimes_n b$.

F.3 *Prop.* Let $n > 1$, $(b \Delta n) = 1$, Nr . Then $\neg (b \Theta_n r) = 0$.

Pf.

If $b = 0$, then $(b \Delta n) = n > 1$, a contradiction. So $\neg b = 0$.

Then proceed by induction, using the fact that $(b \Theta_n r) \otimes_n b = 0$ implies $b \Theta_n r = 0$ by E.5. \square

F.4 *Prop.* $x \Theta_n i = x \Theta_n j \Rightarrow x \Theta_n (i-j) = 1$

G. Euler's Phi Function

G.1 *Prop.* Let $n > 0$. Then, N_k & $M_k, \{x : x \leq n \ \& \ (x \Delta n) = 1\}$, for some (unique) k .

Pf.

$\{x : x \leq n \ \& \ (x \Delta n) = 1\} \subseteq [1 _ n]$. But $M_n, [1 _ n]$, so the result follows by II.E.17. \square

G.2 *Def.* For $n > 0$, let $\phi(n)$ refer to the k assured by the previous proposition.

So, $M_{\phi(n)}, \{x : 0 < x \ \& \ x \leq n \ \& \ (x \Delta n) = 1\}$ for all n with $n > 0$.

Evidently, if 1 exists, then $\phi(1) = 1$.

Recall that $\pi(p)$ is used to say that “ p is prime”.

G.3 *Prop.* $\pi(p) \Leftrightarrow \phi(p) = p-1$.

G.4 *Prop (Euler)* Let $n > 0$, $(a \Delta n) = 1$. Then $a \Theta_n \phi(n) = 1$.

Pf.

Set $k = \phi(n)$, and let a_1, a_2, \dots, a_k be the (non-zero) natural numbers $\leq n$ which are relatively prime to n , i.e. such that $(a_i \Delta n) = 1$.

We claim that

$$a_1 \otimes_n a, a_2 \otimes_n a, \dots, a_k \otimes_n a$$

are just the numbers a_1, a_2, \dots, a_k , perhaps in a different order. It suffices

to establish that, for each i , $1 \leq i \leq k$,

(1) $(a_i \otimes_n a \Delta n) = 1$; and

(2) The a_i are distinct.

(1) follows from E.12, and (2) follows from E.6. \square

G.5 *Corollary (Fermat)*. Let $\pi(p)$, $(a \Delta p) = 1$. Then $a \Theta_p (p-1) = 1$.

G.6 *Corollary*. Let $\pi(p)$, Na . Then $a \Theta_p p = a$.

H. Quadratic Residues

The development in Hardy & Wright, *An Introduction to the Theory of Numbers*, has been followed in this section.

H.1 *Def*. $\pi^*(p)$ if and only if $\pi(p) \ \& \ -p = 2$.

I.e. $\pi^*(p)$ if and only if p is an odd prime. Remark that the supposition that p is an odd prime implies that 3 exists.

H.2 *Def*. $\text{Res}(a,p)$ if and only if $\pi^*(p) \ \& \ (a \Delta p) = 1 \ \& \ \exists x (x \otimes_p x) = a$.

Note: $\text{Res}(a,p)$ implies that a is non-zero. So evidently x may be assumed to be non-zero and $< p$.

H.3 *Prop*. Let $\text{Res}(a,p)$. Then there are precisely two x , with $0 < x < p$, such that $(x \otimes_p x) = a$. Indeed, if x is one, then $(p-x)$ is the other, and

$$x \otimes_p (p-x) = p-a.$$

Pf:

$z \otimes z = a$ for some z , with $0 < z < p$. By E.3.13, $(p-z)$ is another solution. Since $a > 0$, by E.3.14, $z \otimes_p (p-z) = p-a$.

Now suppose $y \otimes y = a$, with $0 < y < p$. WLOG $y \leq z$. By standard manipulation,

$$(z \oplus (p-y)) \otimes (z \oplus y) = 0.$$

By E.5 either $(z \oplus (p-y)) = 0$ or $(z \oplus y) = 0$, i.e. $z = y$ or $z = p-y$. \square

H.4. *Def.* Suppose Nk , $n > 0$. Define $(k!)_n = n \prod_{i=1}^k r_i$, where $r_i = i$ for all $i \leq k$.

$(0!)_n = (1!)_n = 1$, for all $n > 0$.

$(3!)_{10} = 6$, while $(3!)_4 = 2$.

H.5 *Prop.* Let $\pi^*(p)$, $(a \Delta p) = 1$. Set p' such that $2^*p' = p-1$. Then:

1) If $\text{Res}(a,p)$, then $((p-1)!)_p = p - (a \Theta_p p')$

2) If $\neg \text{Res}(a,p)$, then $((p-1)!)_p = a \Theta_p p'$

Pf:

By H.3, for each i with $1 \leq i \leq (p-1)$, there exists i' , also with $1 \leq i' \leq (p-1)$ such that

$$i \otimes_p i' = a.$$

1) By H.3 there are precisely two x , with $1 \leq x \leq (p-1)$, such that $x \otimes_p x = a$.

Call these y and z . Then $y \otimes_p z = p-a$.

Thus the numbers between 1 and $(p-1)$ are either: y , or z , or one of $(p-3)/2$ pairs (i,i') such that $(i \otimes_p i') = a$. But then, setting $p'' = (p-3)/2$

$$\begin{aligned} ((p-1)!)_p &= (p-a) \otimes_p (a \Theta_p p'') \\ &= p - a \otimes_p (a \Theta_p p'') \text{ by E.3.14} \\ &= p - (a \Theta_p p') \end{aligned}$$

2) Then the numbers between 1 and $(p-1)$ are just one of $(p-1)/2$ pairs (i,i') such that $i \otimes_p i' = a$. But then,

$$((p-1)!)_p = a \Theta_p p'$$

\square

H.6 *Corollary (Wilson's Theorem).* Let $\pi(p)$. Then $((p-1)!)_p = p-1$.

Pf:

If $\pi^*(p)$, set $a = 1$ in the previous proposition. \square

H.7 *Corollary.* Let $\pi^*(p)$, $(a \Delta p) = 1$. Set p' such that $2^*p' = p-1$.

- 1) If $\text{Res}(a,p)$, then $a \Theta_p p' = 1$
- 2) If $\neg \text{Res}(a,p)$, then $a \Theta_p p' = p-1$.

H.8 *Lemma.* Let $\pi^*(p)$, $(a \Delta p) = 1$. Set p' such that $2^*p' = p-1$. Consider

$$X = \{x : \exists i (0 < i \leq p' \ \& \ x = i \otimes_p a \ \& \ x > p')\},$$

$$Y = \{y : \exists i (0 < i \leq p' \ \& \ y = i \otimes_p a \ \& \ y \leq p')\}$$

$$Z = \{z : \exists x (Xx \ \& \ z = p - x)\}$$

Then $(Y \cup Z) \equiv [1 _ p']$, i.e. the numbers between (inclusive) 1 and p' .

Pf:

Clearly $(Y \cup Z) \subseteq [1 _ p']$.

Let $z \in Z$, say $z = p - k \otimes_p a$, where $0 < k \leq p'$. We claim that, for all i with $0 < i \leq p'$, $\neg i \otimes_p a = z$. For suppose to the contrary that $i \otimes_p a = z$, with $0 < i \leq p'$. Then

$$(i \otimes_p a) \oplus_p (k \otimes_p a) = 0$$

$$(i \oplus_p k) \otimes_p a = 0 \text{ by E.3.10}$$

$$i \oplus_p k = 0 \text{ by E.5}$$

But this is impossible since $0 < i, k \leq p'$.

Moreover, by the usual argument, the $(i \otimes_p a)$ of X and Y are all distinct, so the elements $(p - x)$ of Z are also distinct. Hence, $(Y \cup Z)$ has p' members, and by the Pigeon Hole Principle II.E.10, $(Y \cup Z) \equiv [1 _ p']$.

□

H.9 *Gauss' Lemma.* Let $\pi^*(p)$, $(a \Delta p) = 1$. Set p' such that $2^*p' = p-1$, and set

$$X = \{x : \exists i (0 < i \leq p' \ \& \ x = i \otimes_p a \ \& \ x > p')\}$$

and suppose Mn, X . Then:

$\text{Res}(a,p)$ if and only if $2 \mid n$.

Pf:

Set,

$$Y = \{y : \exists i (0 < i \leq p' \ \& \ y = i \otimes_p a \ \& \ y \leq p')\}$$

$$Z = \{z : \exists x (Xx \ \& \ z = p - x)\}$$

By lemma H.8, $(Y \cup Z) = [1 - p']$.

If $2 \mid n$, then it is possible to pair off the elements of Z , and so by E.3.13, the product (modulo p) of all the elements of Z equals the product (modulo p) of all the elements of X ,

$$\prod_{Z} z = \prod_{X} x$$

And if $-2 \mid n$, then all but one element of Z can be paired off, so by E.3.13 and E.3.14,

$$\prod_{Z} z = p - \left(\prod_{X} x \right)$$

Hence, if $2 \mid n$,

$$\begin{aligned} & (p'!)_p \otimes_p (a \Theta_p p') \\ &= (1 \otimes_p a) \otimes_p (2 \otimes_p a) \otimes_p \dots \otimes_p (p' \otimes_p a) \\ &= (p'!)_p \text{ by E.8} \end{aligned}$$

Thus $a \Theta_p p' = 1$, so by H.5, $Res(a,p)$. On the other hand, if $-2 \mid n$,

$$\begin{aligned} & (p'!)_p \otimes_p (a \Theta_p p') \\ &= p - (1 \otimes_p a) \otimes_p (2 \otimes_p a) \otimes_p \dots \otimes_p (p' \otimes_p a) \\ &= p - (p'!)_p, \text{ again by E.8.} \end{aligned}$$

Thus $a \Theta_p p' = p - 1$, so by H.5 $-Res(a,p)$.

□

I. The Product Quotient

By the Division Algorithm II.G.3, given any $n \geq 1$ and any c s.t. Nc , there exist q, r s.t.

$$c = q*n + r \text{ where } 0 \leq r < n.$$

One perspective on congruence multiplication is that $(a \otimes_n b)$ is the remainder r of $c = (a * b)$ divided by n should c exist - and in some sense even when c does not. Let us try to put the quotient q in this same light. If either a or $b \leq n$, then the quotient q of $(a*b)$ divided by n is less than

$\max(a,b)$. And so it is determined by a , b , and n even should $(a*b)$ not exist. (Of course if both $a,b > n$, then the quotient may be greater than all of a , b , and n , and so it cannot be supposed to exist.)

That is, define:

I.1 *Def.* Let $n \geq 1$ & Na & $b \leq n$. Use $[a,b / n]$ to refer to the (evidently unique) y , if it exists, such that

$$\exists r \exists k (Seq0(r,k) \ \& \ r_0 = 0 \ \& \ r_k = y \ \&$$

$$\forall j (j < k \ \& \ (j \otimes_n b) + b < n \Rightarrow r_{j+1} = r_j)$$

$$\forall j (j < k \ \& \ \neg (j \otimes_n b) + b < n \Rightarrow r_{j+1} = r_j + 1))$$

Example.

$$[0,6 / 11] = 0$$

$$[1,6 / 11] = [0,6 / 11] = 0, \text{ since } (0 \otimes_{11} 6) + 6 = 6, \text{ which is } < 11$$

$$[2,6 / 11] = [1,6 / 11] + 1 = 1, \text{ since } (1 \otimes_{11} 6) + 6 = 12, \text{ which is } \geq 11$$

(if 12 does not exist, then still $\neg (1 \otimes_{11} 6) + 6 < 11$)

$$[3,6 / 11] = [2,6 / 11] = 1, \text{ since } (2 \otimes_{11} 6) + 6 = (1 + 6) = 7 < 11$$

$$[4,6 / 11] = [3,6 / 11] + 1 = 2 \text{ since } (3 \otimes_{11} 6) + 6 = (7 + 6) = 13 \geq 11$$

So $[a,b / n]$ counts the number of times that adding b to the previous sum puts us to or over n .

I.2 *Prop.* Let $n \geq 1$ & Na & Nb , where $b \leq n$. Then $[a,b / n]$ exists.

Pf:

It suffices to check that r_{j+1} always exists should $j < k$. But an easy induction shows that $r_j \leq j$. Hence $r_{j+1} \leq k$. \square

I.3 *Prop.* Let $n \geq 1$ & $n \geq b$ & Na .

1) $[0, b / n] = 0$.

2) $[a, 0 / n] = 0$.

3) If $a > 0$, then

$$[a,b/n] = \begin{cases} [a-1,b/n] & \text{if } ((a-1) \otimes_n b) + b < n \\ [a-1,b/n]+1 & \text{otherwise} \end{cases}$$

$$4) [1,b/n] = \begin{cases} 0 & \text{if } b < n \\ 1 & \text{if } b = n \end{cases}$$

5) If $a > 0$, then $[(a-1),b/n] \leq [a,b/n] \leq [a-1,b/n] + 1$.

6) If $k > 0$, a is the least number x such that $[x,b/n] = k$ if and only if $[a,b/n] = [a-1,b/n] + 1$.

Pf:

1) By definition.

2) By an easy induction.

3) By the definition of $[a,b/n]$.

4) If $b < n$, then $(0 + b) < n$, so $[1,b/n] = [0,b/n] = 0$, by 1). And if $b = n$, then $(0 + b) = n$, so $[1,b/n] = [0,b/n] + 1 = 1$, again by 1).

5) Follows immediately from 3).

6) Follows immediately from 3).

□

I.4 *Prop.* Let $n \geq 1$ & $n \geq b$ & Na .

1) $a' \leq a \Rightarrow [a',b/n] \leq [a,b/n]$

2) $b \leq n' \leq n \Rightarrow [a,b/n] \leq [a,b/n']$

Pf:

1) By I.3.5.

2) We prove the stronger claim:

$$b \leq n' \leq n \Rightarrow [a,b/n] \leq [a,b/n'] \text{ \& } \\ ([a,b/n] = [a,b/n'] \Rightarrow a \otimes_n b \leq a \otimes_{n'} b)$$

By induction on a . If $a = 0$, then the result holds by I.3.1. Otherwise, suppose true for $(a-1)$. If $[a-1,b/n] < [a-1,b/n']$ then the result follows easily, since $[a,b/n] \leq [a-1,b/n] + 1 \leq [a-1,b/n'] \leq [a,b/n']$, using I.3.5.

So suppose $[a-1,b/n] = [a-1,b/n']$. Then by the induction hypothesis, $(a-1) \otimes_n b \leq (a-1) \otimes_{n'} b$. A consideration of the relevant cases yields the result. □

I.5 *Prop.* Let $a,b,1 \leq n$. Then $[a,b/n] = [b,a/n]$.

Proof:

By a double induction, first on a , then on b . True for $a = 0$, by I.3.1. So suppose true for $(a-1)$. True for $b = 0$, by I.3.2. So suppose true for $(b-1)$.

Set

$$\begin{aligned} x &= [a-1, b-1 / n] \\ y &= (a-1) \otimes_n (b-1). \end{aligned}$$

By the induction hypothesis also

$$x = [b-1, a-1 / n]$$

By E.3.9

$$y = (b-1) \otimes_n (a-1).$$

Now

$$[a, b-1/n] = \begin{cases} x & \text{if } y + (b-1) < n \\ x+1 & \text{otherwise} \end{cases}$$

and

$$[b, a-1/n] = \begin{cases} x & \text{if } y + (a-1) < n \\ x+1 & \text{otherwise} \end{cases}$$

By the induction hypothesis again,

$$[b-1, a / n] = [a, b-1 / n] \text{ and}$$

$$[a-1, b / n] = [b, a-1 / n].$$

Thus:

$$[b, a/n] = \begin{cases} x & \text{if } ((b-1) \otimes_n a) + a < n \ \& \ y + (b-1) < n \\ x+2 & \text{if } \neg ((b-1) \otimes_n a) + a < n \ \& \ \neg y + (b-1) < n \\ x+1 & \text{otherwise} \end{cases}$$

and

$$[a, b/n] = \begin{cases} x & \text{if } ((a-1) \otimes_n b) + b < n \ \& \ y + (a-1) < n \\ x+2 & \text{if } \neg ((a-1) \otimes_n b) + b < n \ \& \ \neg y + (a-1) < n \\ x+1 & \text{otherwise} \end{cases}$$

Hence it suffices to show that the two first pairs of conditions are respectively equivalent.

Note

$$\begin{aligned}(b-1) \otimes_n a &= a \otimes_n (b-1) \\ &= y \oplus_n (b-1)\end{aligned}$$

And suppose

$$(y \oplus_n (b-1)) + a < n \ \& \ y + (b-1) < n.$$

By the second conjunct,

$$y \oplus_n (b-1) = y + (b-1).$$

So

$$y + (b-1) + a < n$$

From this we may conclude both:

$$y + (a-1) + b < n \ \& \ y + (a-1) < n.$$

Again

$$y \oplus_n (a-1) = y + (a-1).$$

Thus

$$(y \oplus_n (a-1)) + b < n \ \& \ y + (a-1) < n.$$

Now assume

$$\neg (y \oplus_n (b-1)) + a < n \ \& \ \neg y + (b-1) < n.$$

By the latter conjunct,

$$y \oplus_n (b-1) = (b-1) - (n-y)$$

Thus

$$\neg ((b-1) - (n-y)) + a < n$$

and

$$(b-1) - (n-y) \text{ exists.}$$

So

$$n-y \leq b-1$$

$$(n-y) + 1 \leq b$$

Suppose

$$y + (a-1) < n.$$

Then:

$$(a-1) < n-y$$

$a \leq (n-y) + 1$ (which exists by the above, being $\leq b$)

Since $a-1 < n-y \leq b-1$

$b > a$.

$b-a \geq b - ((n-y)+1) = (b-1) - (n-y)$

Since $n > b$,

$n > (b - a) + a$

$> ((b-1) - (n-y)) + a$, a contradiction.

Therefore

$\neg y + (a-1) < n$.

So

$y \oplus_n (a-1) = (a-1) - (n-y)$.

Suppose

$(y \oplus_n (a-1)) + b < n$

Then

$((a-1) - (n-y)) + b < n$.

If $b-1 \geq n-y$, then $(b-1) - (n-y)$ exists, so

$((b-1) - (n-y)) + a = ((a-1) - (n-y)) + b < n$,

a contradiction. Thus

$b-1 < n-y$.

$y + (b-1) < n$,

another (and the final) contradiction. \square

I.6 *Prop.* Let $n \geq 1$ & $n \geq b$ & Na .

1) $[b, n/n] = b$

2) $(a+n)$ exists $\Rightarrow [a+n, b/n] = b + [a, b/n]$.

3) $y = q*n + r \Rightarrow [y, b/n] = q*b + [r, b/n]$.

Pf:

1) By induction on b . Holds for $b = 0$ by I.3.1. For $b > 0$, assume true for $(b-1)$. Then

$[b, n/n] = [b-1, n/n] + 1$ by 3),

since there is no x s.t. $(x + n) < n$. So, using the induction hypothesis,

$[b, n/n] = b$.

2) By induction on a . Holds for $a = 0$ by 1). For $a > 0$, assume true for $(a-1)$, and suppose $(a+n+1)$ exists. Then

$$[a+n+1, b/n] = \begin{cases} [a+n, b/n] & \text{if } ((a+n) \otimes_n b) + b < n \\ [a+n, b/n] + 1 & \text{otherwise} \end{cases}$$

and

$$[a+1, b/n] = \begin{cases} [a, b/n] & \text{if } (a \otimes_n b) + b < n \\ [a, b/n] + 1 & \text{otherwise} \end{cases}$$

But $(a+n) \otimes_n b = (a \otimes_n b)$ by E.3.6. The result follows by a consideration of the two pairs of equivalent cases.

3) By induction on q . Obviously holds for $q = 0$. For the induction step use 2).

□

I.7 *Prop.* Let $n \geq 1$ & $n \geq b$ & Na . Suppose (a^*b) exists. Then

$$a^*b = ([a, b/n] * n) + (a \otimes_n b).$$

Moreover, suppose $a^*b = q^n + r$, where Nq and $r < b$. Then $q = [a, b/n]$.

Pf:

By induction on a . For the induction step, note that

$$[a+1, b/n] = \begin{cases} [a, b/n] & \text{if } (a \otimes_n b) + b < n \\ [a, b/n] + 1 & \text{otherwise} \end{cases}$$

Now if $(a \otimes_n b) + b < n$, then $(a+1) \otimes_n b = (a \otimes_n b) + b$; and otherwise $(a+1) \otimes_n b = (a \otimes_n b) - (n - b)$. The first assertion follows by a consideration of cases.

The second assertion follows by the uniqueness condition of the Division Algorithm II.G.3.

□

I.8 *Corollary.* Let $n \geq 1$ & $n \geq b$ & Na . Suppose $(a \otimes_n b)$ is non-zero. Then:

- 1) If (a^*b) exists, then $[a, b/n] * n < a^*b$.
- 2) In particular, if $n > a^*b$, then $[a, b/n] = 0$.
- 3) In particular, if $n > a^*b$, then $[i, b/n] = 0$ for all $i \leq a$.

I.9 *Corollary.* Let $b \geq 1$ & $[a, b/n] \geq 1$ & $n = q^*b + r$, where Nq and $r < b$. Then $a \geq q$, with equality only in the case $r = 0$.

Pf:

Suppose $q^*b = n$. If $a < q$, then (a^*b) exists and $< n$, so $[a, b/n] = 0$ by I.8.2, a contradiction. Hence $a \geq q$.

Now suppose $r > 0$. Then $q^*b < n$, so $[q, b/n] = 0$, again by I.8.2. But then $a > q$.

□

I.10 *Prop.* Let $n = q^*b + r$, where $r < b \leq n$.

1) $a \otimes_n b < r$ if and only if $[a, b/n] = [a+q, b/n]$.

2) If $[a, b/n] = [a+u, b/n] = [a+u+1, b/n] - 1$, then for all i with $0 \leq i \leq u$,
 $(a+i) \otimes_n b = (a \otimes_n b) + (i^*b)$

and

$$(a+u+1) \otimes_n b = (a \otimes_n b) + (u^*b - (n - b))$$

3) If $a \otimes_n b \geq r$, then $[a+q, b/n] = [a, b/n] + 1$.

4) If Na , then $[a+q+1, b/n] \geq [a, b/n] + 1$.

Pf:

Note that $q \geq 1$ since $r < b \leq n$.

1) Suppose $a \otimes_n b < r$. By an easy induction $((a+i) \otimes_n b) + b < n$, for all i where $i \leq q-1$. Thus $[a, b/n] = [a+q, b/n]$.

On the other hand, suppose $a \otimes_n b \geq r$. Suppose for all $i \leq q-1$, that $((a+i) \otimes_n b) + b < n$. Then

$$(a+i+1) \otimes_n b = ((a+i) \otimes_n b) + b$$

for all $i \leq (q-1)$, so in particular $(a+q) \otimes_n b = (a \otimes_n b) + (q^*b) > n$, a contradiction. Hence for some least $j \leq (q-1)$, $\neg ((a+j) \otimes_n b) + b < n$. Then $[a+j+1, b/n] = [a, b/n] + 1$, which implies that $[a+q, b/n] > [a, b/n]$ since $q \geq j+1$.

□

I.11 *Prop.* Let $n, m > 0$, $a \leq m$, and Nk . Then:

$$k \otimes_n a = ([k, a/m] \otimes_n m) \oplus_n (k \otimes_m a)$$

Pf:

By induction on k . If $k = 0$, both sides reduce to 0.

Next, suppose $k \geq 1$, and

$$(k-1) \otimes_n a = ([k-1, a/m] \otimes_n m) \oplus_n ((k-1) \otimes_m a).$$

Adding (modulo n) a to both sides, and using associativity of modulo addition,

$$(k \otimes_n a) = ([k-1, a/m] \otimes_n m) \oplus_n ((k-1) \otimes_m a) \oplus_n a$$

Case 1. $((k-1) \otimes_m a) + a < m$.

Then $[k, a/m] = [k-1, a/m]$, and

$$((k-1) \otimes_m a) \oplus_n a \equiv_n ((k-1) \otimes_m a) + a = k \otimes_m a,$$

whence the result follows.

Case 2. $\neg ((k-1) \otimes_m a) + a < m$.

Then $[k, a/m] = [k-1, a/m] + 1$, and

$$k \otimes_m a = ((k-1) \otimes_m a) - (m - a), \text{ i.e.}$$

$$(k-1) \otimes_m a = (k \otimes_m a) + (m - a)$$

So

$$((k-1) \otimes_m a) \oplus_n a = (k \otimes_m a) \oplus_n m.$$

But

$$\begin{aligned} ([k-1, a/m] \otimes_n m) \oplus_n m &= ([k-1, a/m] \oplus_n 1) \otimes_n m \\ &= [k, a/m] \otimes_n m. \end{aligned}$$

whence the result follows.

□

I.12 *Prop.* Suppose $r \leq b$ & $1 \leq b$ & $1 \leq k$. Then

$$r = ([k, r/b] - [k-1, r/b]) * b + ((k \otimes_b r) - ((k-1) \otimes_b r))$$

Pf:

By I.3.3 there are the following two cases.

Case 1. $[k, r/b] = [k-1, r/b]$.

Then $k \otimes_b r = ((k-1) \otimes_b r) + r$, by I.3.3.

Case 2. $[k, r/b] = [k-1, r/b] + 1$.

Then $k \otimes_b r = ((k-1) \otimes_b r) - (b - r)$, by I.3.3.

□

I.13 *Prop.* Let $n \geq b \geq k \geq 1$, where $\neg b \mid n$. Suppose a is the least number s.t. $[a, b/n] = k$. Then:

- 1) $[n, k/b] = (a-1)$
- 2) $(a \otimes_n b) + (k \otimes_b n) = b$

Pf:

Set $n = q \cdot b + r$, for some q, r where $0 \leq r < b$. In fact, $0 < r$, since by assumption $\neg b \mid n$.

Proceed by induction on k . Consider $k = 1$. Then

$$\begin{aligned} [n, 1/b] &= q + [r, 1/b] \text{ by I.6.3} \\ &= q \text{ by I.3.4} \end{aligned}$$

On the other hand, $[q, b/n] = 0$ by I.8.2 and $[q+1, b/n] = 1$ by I.10.4. Hence $q+1 = a$, whence $[n, 1/b] = a-1$. So 1).

As for 2),

$$0 = (q \otimes_n b) \oplus_n r.$$

Thus $q \otimes_n b = n-r$ by D.4.1. Note $r < b$, so $\neg (n-r) + b \leq n$, and hence

$\neg (q \otimes_n b) + b \leq n$. Thus

$$\begin{aligned} (q+1) \otimes_n b &= (q \otimes_n b) - (n - b) \\ &= (n - r) - (n - b) \\ &= b - r \end{aligned}$$

So

$$\begin{aligned} (a \otimes_n b) + (1 \otimes_b n) &= ((q+1) \otimes_n b) + r \\ &= (b - r) + r \\ &= b. \end{aligned}$$

Now suppose true for $(k-1)$, and suppose a is the least number such that $[a, b/n] = k$. Let u be such that $(a-u)$ is the least number x such that $[x, b/n] = (k-1)$. Then $[a-u, b/n] = k-1$, and by the induction hypothesis

$$\begin{aligned} [n, k-1/b] &= a-u-1 \\ ((a-u) \otimes_n b) + ((k-1) \otimes_b n) &= b. \end{aligned}$$

Remark by I.9 $a \geq q$.

Claim. Either:

- (i) $u = q$ & $(a-u) \otimes_n b \geq r$
- (ii) $u = q+1$ & $(a-u) \otimes_n b < r$

Pf of Claim:

Suppose $u < q$. Then $[a-q, b/n] \leq [a-u, b/n] = k-1$. Since $(a-u)$ is least, this implies that $[a-q, b/n] = k-2$. But I.10.1 and I.10.3 imply that $[(a-q)+q, b/n]$ equals $(k-2)$ or $((k-2) + 1)$, contradicting the fact that $[a, b/n] = k$.

Suppose $u > q+1$. Then $a > (a-u) + (q+1)$. But
 $k = [a, b/n] \geq [(a-u) + (q+1), b/n]$ by I.4.1

and

$$[(a-u) + (q+1), b/n] \geq [a-u, b/n] + 1 = k \text{ by I.10.4.}$$

So $[(a-u) + (q+1), b/n] = k$, contradicting the leastness of a .

Finally, note that by I.10.1, $(a-u) \otimes_n b < r$ if and only if $[a-u, b/n] = [(a-u)+q, b/n]$. Since $[a-1, b/n] < [a, b/n]$, we must have that $u = q+1$ if and only if $[a-u, b/n] = [(a-u)+q, b/n]$.

Now

$$[n, k-1/b] = q*(k-1) + [r, (k-1)/b]$$

and

$$[n, k/b] = q*k + [r, k/b]$$

So,

$$\begin{aligned} [n, k/b] &= [n, k-1/b] + q + ([r, k/b] - [r, (k-1)/b]) \\ &= (a - u - 1) + q + ([k, r/b] - [(k-1), r/b]) \end{aligned}$$

Recall

$$((a-u) \otimes_n b) + ((k-1) \otimes_b n) = b$$

So

$$((a-u) \otimes_n b) + ((k-1) \otimes_b r) = b$$

Thus

$$\begin{aligned} (a-u) \otimes_n b < r &\Leftrightarrow (k-1) \otimes_b r > b - r. \\ &\Leftrightarrow -((k-1) \otimes_b r) + r < b \\ &\Leftrightarrow [k, r/b] = [k-1, r/b] + 1 \end{aligned}$$

Hence either:

$$u = q \ \& \ ([k, r/b] - [(k-1), r/b]) = 0$$

or

$$u = q+1 \ \& \ ([k, r/b] - [(k-1), r/b]) = 1.$$

A consideration of the cases leads to

$$[n, k/b] = a-1.$$

Finally, it needs to be shown that

$$(a \otimes_n b) + (k \otimes_b n) = b,$$

or equivalently, since $n \equiv r \pmod{b}$,

$$(a \otimes_n b) + (k \otimes_b r) = b,$$

Now by I.10.2

$$a \otimes_n b = ((a-u) \otimes_n b) + ((u-1)*b - (n-b)).$$

and by I.12

$$k \otimes_b r = (r + ((k-1) \otimes_b r)) - ([k, r/b] - [(k-1), r/b]) * b$$

Adding and using the induction hypothesis $((a-u) \otimes_n b) + ((k-1) \otimes_b n) = b$,

$$\begin{aligned} & (a \otimes_n b) + (k \otimes_b r) \\ &= r + u*b - (n-b) - ([k, r/b] - [(k-1), r/b]) * b \end{aligned}$$

If $[k, r/b] - [(k-1), r/b] = 0$, then $u = q$; while if $[k, r/b] - [(k-1), r/b] = 1$, then $u = q+1$. A consideration of both cases results in

$$(a \otimes_n b) + (k \otimes_b r) = b.$$

□

The next proposition could be proven in greater generality, but the form given suffices for our needs in the proof of Quadratic Reciprocity.

I.14 *Prop.* If $a > b$ and $n = 2*a + 1$, then

$$[a, 2*b + 1 / n] = b.$$

Pf:

We will prove the stronger claim, that

$$a > b \ \& \ n = 2*a + 1 \Rightarrow [a, 2*b + 1 / n] = b \ \& \ (2*b + 1) \otimes_n a = a - b.$$

Proceed by induction on b . For the case $b = 0$, note that $[a, 1/n] = 0$ by I.8.2, and that $1 \otimes_n a = a$.

Suppose so for $(b-1)$, and let $a > b \ \& \ n = 2*a + 1$. Then $a > (b-1)$, so

$$\begin{aligned} & [a, 2*(b-1) / n] = (b-1) \\ & \ \& \ (2*b - 1) \otimes_n a = a - (b - 1). \end{aligned}$$

Then

$$((2*b - 1) \otimes_n a) + a = 2*a - (b - 1) < 2*a + 1 = n.$$

Hence

$$(2^*b) \otimes_n a = 2^*a - (b - 1)$$

and

$$\begin{aligned} [2^*b, a / n] &= [2^*b - 1, a/n] \\ &= [a, 2^*b - 1, a/n] \text{ by I.5} \\ &= b \text{ by the Induction Hypothesis} \end{aligned}$$

And since $a > b$,

$$- 3^*a - (b - 1) < n.$$

Hence

$$\begin{aligned} (2^*b + 1) \otimes_n a &= 2^*a - (b - 1) - (n - a) \\ &= 2^*a - (b - 1) - (a + 1) \\ &= a - b \end{aligned}$$

and

$$\begin{aligned} [2^*b + 1, a / n] &= [2^*b, a / n] + 1 \\ &= b + 1. \end{aligned}$$

□

J. Quadratic Reciprocity

J.1 Prop. Let $\pi^*(p)$, $(a \Delta p) = 1$, $- 2 \mid a$. Set p' such that $2^*p' = p-1$. Then

$\text{Res}(a,p)$ if and only if $(2 \sum_{k=1}^{p'} [k, a/p]) \equiv_2 0$

(Recall the “2” before the summation sign means that one is adding modulo 2. It will be dropped for the proof, and any modulo not specified is assumed to be modulo 2.)

Pf:

By I.11, where $1 \leq k \leq p'$,

$$k \otimes_2 a = ([k, a/p] \otimes_2 p) \oplus_2 (k \otimes_p a)$$

p is odd, so $p \equiv 1$. Thus

$$\sum_{k=1}^{p'} k \equiv \sum_{k=1}^{p'} [k, a/p] \oplus_2 \sum_{k=1}^{p'} (k \otimes_p a).$$

But by H.8, $[1 - p']$ are just the numbers $(i \otimes_p a)$ and $(p - (j \otimes_p a))$, where

$0 < i \leq p' \& i \otimes_p a \leq p'$ and

$0 < j \leq p' \& j \otimes_p a > p'$.

So, summing up these numbers mod 2 (we'll use I and J, to indicate the restriction on the indices),

$$\sum_I (i \otimes_p a) \oplus_2 \sum_J (p - (j \otimes_p a)) = \sum_{k=1}^{p'} [k, a/p] \oplus_2 \sum_{k=1}^{p'} (k \otimes_p a)$$

Thus

$$\sum_J p = \sum_{k=1}^{p'} [k, a/p] \oplus_2 \sum_{k=1}^{p'} (2 \otimes_2 (k \otimes_p a))$$

This last term equals 0, so

$$\sum_J p = \sum_{k=1}^{p'} [k, a/p]$$

Since $p = 1$, the term on the left-hand-side is 0 if the number of j is even, 1 otherwise. By Gauss' Lemma, this means that the term on the left-hand-side is 0 if $\text{Res}(a, p)$, 1 otherwise. \square

J.2 *Lemma.* Let $\pi^*(p), \pi^*(q), p > q$. Set p', q' such that $2^*p' = p-1$ and $2^*q' = q-1$. Then

$$p' \otimes_2 q' = \sum_{i=1}^{p'} [q, i/p] \oplus_2 \sum_{i=1}^{q'} [p, i/q]$$

Note: all \sum summations are sums modulo 2.

Pf:

We will show by induction that, for all $k, 1 \leq k < p$,

$$\sum_{i=1}^k [q, i/p] \oplus_2 \sum_{i=1}^{f(k)} [p, i/q] = k \otimes_2 f(k),$$

where $f(k) = [k, q/p]$. This suffices, since we may set $k = p'$ (being $< p$), and $f(p') = q'$ by I.14.

Let $k = 1$. Set $q = u^*p + v$, where Nu and $v < p$. Remark, since p and q are distinct primes, that $v > 0$, so $q > u^*p$. Then

$$f(1) = [1, q/p] = 0 \text{ by I.3.4.}$$

So,

$$\sum_{i=1}^{f(1)} [p, i/q] = 0.$$

But

$$[q, 1/p] = [1, q/p] = f(1) \equiv_2 1 \otimes_2 f(1).$$

Thus the claim holds when $k = 1$.

Now let $k > 1$, and suppose the claim holds for $(k-1)$. Then:

$$\sum_{i=1}^{k-1} [q, i/p] \oplus_2 \sum_{i=1}^{f(k-1)} [p, i/q] = (k-1) \otimes_2 f(k-1).$$

Case 1. $f(k) = f(k-1)$.

Then the claim follows by adding, modulo 2, $f(k) = f(k-1) = [q, k/p]$ to both sides.

Case 2. $f(k) = f(k-1) + 1$.

That is, $[k, q/p] = [k-1, q/p] + 1$, so k is the least number x such that $[x, q/p] = f(k)$. By I.13, $[p, f(k)/q] = k-1$. Adding $f(k) \oplus_2 [p, f(k)/q]$ to both sides, the left-hand side becomes

$$\sum_{i=1}^k [q, i/p] \oplus_2 \sum_{i=1}^{q'} [p, i/q],$$

while the right-hand side, given that $[p, f(k), q] = k-1$, becomes

$$\begin{aligned} & ((k-1) \otimes_2 f(k-1)) \oplus_2 f(k) \oplus_2 (k-1) \\ &= ((k-1) \otimes_2 (f(k-1) + 1)) \oplus_2 f(k) \\ &= ((k-1) \otimes_2 f(k)) \oplus_2 f(k) \end{aligned}$$

$$= k \otimes_2 f(k)$$

□

J.3 *Theorem of Quadratic Reciprocity (Gauss)*. Let $\pi^*(p), \pi^*(q), -p = q$. Then $(\text{Res}(p,q) \Leftrightarrow \text{Res}(q,p)) \Leftrightarrow p \equiv_4 1 \vee q \equiv_4 1$.

Pf.

WLOG suppose $p > q$.

By J.1 it suffices to show that

$$\sum_{k=1}^r [k, q/p] \equiv_2 \sum_{k=1}^s [k, p/q] \Leftrightarrow (p \equiv_4 1 \text{ or } q \equiv_4 1),$$

where $(2^*r) = p-1$ and $(2^*s) = q-1$.

Now

$$\sum_{k=1}^r [k, q/p] \equiv_2 \sum_{k=1}^s [k, p/q] \Leftrightarrow \sum_{k=1}^r [k, q/p] \oplus_2 \sum_{k=1}^s [k, p/q] = 0$$

.

$$\Leftrightarrow r \otimes_2 s = 0 \text{ by J.2}$$

$$\Leftrightarrow p \equiv_4 1 \vee q \equiv_4 1.$$

□

K. Conclusion

The proof of Quadratic Reciprocity confirms the power of **F**. The *ad infinitum* principle may make easier some mathematical manipulation, but more and more, it looks like it does not, in any genuine sense of the term, extend our mathematical knowledge. Nonetheless, more research, and in

particular more proofs of more theorems, still needs still to be conducted, before the conclusion can be asserted with any vigor.