Appendix A

Primitive Elements and Quadratic Residues

This mathematical appendix treats in a closed form some number theoretic subjects that play a major role for cryptology. They relate to the multiplicative group of a residue class ring.

As we saw in the main text several results on the security of cryptographic procedures depend on the non-existence of efficient algorithms for some tasks.

Relevant problems and their (incomplete) solutions are:

1. Find a primitive element.
   - The complexity of the general case is unknown.
   - Exhaustion is efficient if ERH holds.
   - There is a much more efficient probabilistic algorithm, that however doesn't even terminate in the worst case.
   - For many prime modules the solution is trivial.
   - Proving primitivity is efficient if the prime factors of the order of the multiplicative group are known. Otherwise the complexity is unknown.
   - For a composite module the problem reduces to its prime factors—if these are known.
2. Decide on quadratic residuosity.
   - For prime modules there is an efficient algorithm.
   - For a composite module the problem reduces to its prime factors—if these are known.
   - For composite modules with unknown prime factors the complexity is unknown. Presumably the problem is hard (as hard as prime decomposition).

3. Find a quadratic non-residue.
    - The complexity of the general case is unknown.
    - Exhaustion is efficient if ERH holds.
    - There is an efficient probabilistic algorithm, that however doesn't even terminate in the worst case.
    - For most primes the solution is trivial.
    - For a composite module the problem reduces to its prime factors—if these are known.

A related problem, finding square roots in residue class rings, is treated in Chapter 5.

A.1 Primitive Elements for Powers of 2

The cases $n = 2$ or 4 are trivial: $\mathbb{M}_2$ is the one-element group. $\mathbb{M}_4$ is cyclic of order 2, thus $3 \equiv -1 \pmod 4$ is primitive.

From now on we assume $n = 2^e$ with $e \geq 3$. Note that $\mathbb{M}_n$ consists of the residue classes of the odd integers, hence $\varphi(n) = 2^{e-1}$.

Lemma 10 *Let $n = 2^e$ with $e \geq 2$.*

(i) *If a is odd, then*

$$a^{2^s} \equiv 1 \pmod{2^{s+2}} \quad \textit{for all } s \geq 1.$$

(ii) *If $a \equiv 3 \pmod 4$, then $n \mid 1 + a + \cdots + a^{n/2-1}$.*

Proof. (i) First we prove the statement for $s = 1$. In the case $a = 4q + 1$ we have $a^2 = 16q^2 + 8q + 1$. In the case $a = 4q + 3$ we have $a^2 = 16q^2 + 24q + 9$, hence $a^2 \equiv 1 \pmod 8$.

The assertion for general s follows by induction:

$$a^{2^{s-1}} = 1 + t2^{s+1} \Longrightarrow a^{2^s} = (a^{2^{s-1}})^2 = 1 + 2t2^{s+1} + t^2 2^{2s+2}.$$

(ii) By (i) we have $2n = 2^{e+1} \mid a^{n/2} - 1$. Since only the first power of 2 divides $a - 1$ we conclude

$$n = 2^e \mid \frac{a^{n/2} - 1}{a - 1}$$

as claimed. $\diamond$

Lemma 11 *Let p a prime and e an integer with $p^e \geq 3$. Let p^e be the largest power of p that divides $x - 1$. Then p^{e+1} is the largest power of p that divides $x^p - 1$.*

Proof. We have $x = 1 + tp^e$ with an integer t that is not a multiple of p. The binomial theorem yields

$$x^p = 1 + \sum_{k=1}^{p} \binom{p}{k} t^k p^{ke}.$$

Since p divides all binomial coefficients $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $k = 1, \ldots, p-1$ we can factor out p^{e+1} from the sum:

$$x^p = 1 + tp^{e+1}s$$

with some integer s. Hence p^{e+1} divides $x^p - 1$. It remains to show that s is not a multiple of p. We take a closer look at s:

$$\begin{aligned} s &= \sum_{k=1}^{p} \frac{1}{p}\binom{p}{k} \cdot t^{k-1}p^{e(k-1)} \\ &= 1 + \frac{1}{p}\binom{p}{2} \cdot tp^e + \cdots + \frac{1}{p} \cdot t^{p-1}p^{e(p-1)}. \end{aligned}$$

Since $p^e \geq 3$ we have $e(p-1) \geq 2$, hence $s \equiv 1 \pmod p$. $\diamond$

Lemma 10 implies

$$a^{2^{e-2}} \equiv 1 \pmod n \quad \text{for all odd } a.$$

Hence the exponent $\lambda(n) \leq 2^{e-2}$, and $\mathbb{M}_n$ is not cyclic. More exactly:

Proposition 17 *Let $n = 2^e$ with $e \geq 3$. Then:*

(i) *The order of -1 in $G = \mathbb{M}_n$ is 2, the order of 5 is 2^{e-2}, and G is the direct product of the cyclic groups generated by -1 and 5.*

(ii) *If $e \geq 4$, then the primitive elements $\bmod n$ are the integers $a \equiv 3, 5 \pmod 8$. Their number is $n/4$.*

Proof. (i) Since $\operatorname{ord} 5 \mid 2^e$ and $\operatorname{ord} 5 \leq 2^{e-2}$, we conclude that $\operatorname{ord} 5$ is a power of 2 and $\leq 2^{e-2}$.

Now 2^2 is the largest power of 2 in $5 - 1$, thus 2^3 is the largest power of 2 in $5^2 - 1$ (by Lemma 11). Successively we conclude that 2^{e-1} is the largest power of 2 in $5^{2^{e-3}} - 1$. Hence the 2^{e-2}-th power of 5 is the smallest one $\equiv 1 \pmod{2^e}$.

The product of the two subgroups is direct since -1 is not a power of 5—otherwise $5^k \equiv -1 \pmod n$, and, because of $e \geq 2$, also $5^k \equiv -1 \pmod 4$, contradicting $5 \equiv 1 \pmod 4$.

The direct product is all of G since its order is $2 \cdot 2^{e-2}$.

(ii) By (i) each element $a \in G$ has a unique expression of the form $a = (-1)^r 5^s$ with $r = 0$ or 1, and $0 \leq s < 2^{e-2}$. Hence a^k equals 1 in $\mathbb{Z}/n\mathbb{Z}$ if and only if kr is even and ks is a multiple of 2^{e-2}. In particular then k is even. If s is even, then the condition is satisfied for some $k < 2^{e-2}$. Thus a is primitive if and only if s is odd, or equivalently $a \equiv \pm 5 \pmod 8$. $\diamond$

As a corollary we have $\lambda(2^e) = 2^{e-2}$ for $e \geq 4$, and $\lambda(8) = 2$.

A.2 Primitive Elements for Prime Modules

More difficult (and mathematically more interesting) is the search for primitive elements for a prime module. Since the multiplicative group is cyclic it suffices to find *one* primitive element—all the other ones are powers of it with exponents coprime with $p-1$. In particular there are exactly $\varphi(p-1)$ primitive elements $\bmod p$. Usually the primitive elements for any module n where $\mathbb{M}_n$ is cyclic are also called **primitive roots** $\bmod n$.

The simplest, but not best, method is trying $x = 2, 3, 4, \ldots$, and testing if $x^d \neq 1$ for each proper divisor d of $p-1$. We need not to test all divisors:

Lemma 12 *Let p be a prime ≥ 5. An integer x is primitive* $\bmod p$, *if and only if $x^{(p-1)/q} \neq 1$ in $\mathbb{F}_p$ for each prime factor q of $p-1$.*

Proof. The order of x divides $p-1$, and each proper divisor of $p-1$ divides at least one of the quotients $\frac{p-1}{q}$. $\diamond$

To apply this criterion we need the prime decomposition of $p-1$. Then the test is efficient: The number of prime factors is $\leq \log_2(p-1)$, and for each of them we apply the binary power algorithm.

Example For $p = 41$ we have $p - 1 = 40 = 2^3 \cdot 5$. Hence x is primitive if and only if $x^{20} \neq 1$ and $x^8 \neq 1$. The test runs through the following steps in $\mathbb{F}_{41}$:

$$\begin{array}{llll}
x = 2: & x^2 = 4, & x^4 = 16, & \begin{cases} x^8 = 10, \\ x^{20} = x^8x^8x^4 = 1. \end{cases} \\
x = 3: & x^2 = 9, & x^4 = 81, & x^4 = -1, \;\; x^8 = 1. \\
x = 4: & x = 2^2, & \text{hence} & x^{20} = 1. \\
x = 5: & x^2 = 25, & x^4 = 10 & \begin{cases} x^8 = 18, \\ x^{20} = x^8x^8x^4 = 1. \end{cases} \\
x = 6: & x^2 = 36, & x^4 = 25 & \begin{cases} x^8 = 10, \\ x^{20} = x^8x^8x^4 = -1. \end{cases}
\end{array}$$

Hence 6 *is a primitive root for $p = 41$.*

The obvious question is how many integers must we try to find a primitive root? The quantity

$$\alpha(p) := \min\{x \in \mathbb{N} \mid x \text{ is primitive for } p\}$$

measures the complexity of complete search (but neglects the complexity of the proof of primitivity). It is known that the the function α is not bounded. In 1962 Burgess proved

$$\alpha(p) = \mathrm{O}(\sqrt[6]{p}).$$

Assuming ERH this exponential bound may be lessened to a polynomial one. The best known result is by Shoup 1990:

$$\alpha(p) = \mathrm{O}(\log(p)^6(1 + \log\log(p))^4).$$

Even completely simple questions are yet unanswered:

- Is 2 primitive for infinitely many primes?
- Is 10 primitive for infinitely many primes? (Gauss' conjecture)

Artin more generally conjectured: If $a \in \mathbb{N}$, and a is not an integer square (i. e. $a \neq 0, 1, 4, 9, \ldots$), then a is primitive for infinitely many primes.

Some relevant references:

- D. R. Heath-Brown: Artin's conjecture for primitive roots. Quart. J. Math. Oxford 37 (1986), 27–38.
- M. Ram Murty: Artin's conjecture for primitive roots. Math. Intelligencer 10 (1988), 59–67.
- V. Shoup: Searching for primitive roots in finite fields. Proc. 22nd STOC 1990, 546–554.
- Murata: On the magnitude of the least prime primitive root. J. Number Theory 37 (1991), 47–66.

A.3 Primitive Elements for Prime Powers

For prime powers we need one more lemma.

Lemma 13 *Let p be prime ≥ 3, k, an integer, and $d \geq 0$. Then*

$$(1+kp)^{p^d} \equiv 1 + kp^{d+1} \pmod{p^{d+2}}.$$

Proof. For $d = 0$ the statement is trivial. For $d \geq 1$ we reason by induction: Assume

$$(1+kp)^{p^{d-1}} = 1 + kp^d + rp^{d+1} = 1 + (k+rp)p^d.$$

Then

$$(1+kp)^{p^d} = (1+(k+rp)p^d)^p \equiv 1+p\cdot(k+rp)\cdot p^d \equiv 1+kp^{d+1} \pmod{p^{d+2}},$$

since $d + 2 \leq 2d + 1$ and $p \geq 3$. $\diamond$

Proposition 18 *Let p be prime ≥ 3, e, an exponent ≥ 2, and a be primitive* $\bmod\, p$. *Then:*

(i) *a generates the group $\mathbb{M}_{p^e}$ if and only if $a^{p-1} \bmod p^2 \neq 1$.*

(ii) *a or $a+p$ generates $\mathbb{M}_{p^e}$.*

(iii) *$\mathbb{M}_{p^e}$ is cyclic, and $\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$.*

Proof. (i) Let t be the multiplicative order of $a \bmod p^e$, necessarily a multiple of the order of $a \bmod p$, hence of $p-1$. On the other hand t divides $\varphi(p^e) = p^{e-1}(p-1)$. Hence $t = p^d(p-1)$ with $0 \leq d \leq e-1$.

Choose k such that $a^{p-1} = 1 + kp$. Then by Lemma 13

$$(a^{p-1})^{p^{e-2}} \equiv 1 + kp^{e-1} \equiv 1 \pmod{p^e} \iff p|k \iff a^{p-1} \equiv 1 \pmod{p^2}.$$

This is *not* the case if and only if $d = e-1$.

(ii) Assume a doesn't generate $\mathbb{M}_{p^e}$. Then $a^{p-1} \equiv 1 \pmod{p^2}$, hence

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 - a^{p-2} \pmod{p^2},$$

and this is not $\equiv 1 \pmod{p^2}$.

(iii) follows immediately from (ii). $\diamond$

We immediately get an analogous result for modules that are twice a prime power:

Corollary 1 *Let $q = p^e$ be a power of a prime $p \geq 3$. Then:*

(i) *The multiplicative group* $\mathbb{M}_{2q}$ *is canonically isomorphic with* $\mathbb{M}_q$*, hence cyclic.*

(ii) *If* a *is a primitive element* $\bmod q$*, then* a *is primitive* $\bmod 2q$ *for odd* a*, and* $a + q$ *is primitive* $\bmod 2q$ *for even* a*.*

(iii) $\lambda(2p^e) = p^{e-1}(p-1)$.

Proof. (i) Since q and 2 are coprime, and $\mathbb{M}_2$ is the trivial group, by the chinese remainder theorem $\mathbb{M}_{2q} \cong \mathbb{M}_2 \times \mathbb{M}_q \cong \mathbb{M}_q$. This map is explicitely given by $a \bmod 2q \mapsto a \bmod q$.

(ii) Exactly one of a and $a+q$ is odd, hence coprime with $2q$. Thus the inverse isomorphism is

$$a \mapsto \begin{cases} a, & \text{if } a \text{ is odd,} \\ a+q, & \text{if } a \text{ is even.} \end{cases}$$

(iii) obvious. $\diamond$

A.4 The Structure of the Multiplicative Group

The previous results allow a complete characterization of the modules n for which the multiplicative group $\mathbb{M}_n$ is cyclic:

Corollary 2 (Gauss 1799) *For $n \geq 2$ the multiplicative group $\mathbb{M}_n$ is cyclic if and only if n is one of the integers 2, 4, p^e, or $2p^e$ with an odd prime p.*

Proof. This follows from Proposition 18, Corollary 1, and the following Lemma 14. $\diamond$

Lemma 14 *If $m, n \geq 3$ are coprime, then $\mathbb{M}_{mn}$ is not cyclic, and $\lambda(mn) < \varphi(mn)$.*

Proof. If $n \geq 3$, then $\varphi(n)$ is even. For a prime power this follows from the explicit formula. In the general case we reason by the multiplicativity of the φ-function. We conclude

$$\mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(m)\,\varphi(n) = \varphi(mn),$$

$$\lambda(mn) = \mathrm{kgV}(\lambda(m), \lambda(n)) \leq \mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(mn).$$

Hence $\mathbb{M}_{mn}$ is not cyclic. $\diamond$

Now the structure of the multiplicative group is completely known also for a general module. Let us denote the cyclic group of order d by $\mathcal{Z}_d$.

Theorem 2 *Let $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of the integer $n \geq 2$ with different odd primes $p_1, \ldots, p_r$, and $e \geq 0$, $r \geq 0$, $e_1, \ldots, e_r \geq 1$. Let $q_i = p_i^{e_i}$ and $q_i' = p_i^{e_i - 1}(p_i - 1)$ for $i = 1, \ldots, r$. Then*

$$\mathbb{M}_n \cong \begin{cases} \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{if } e = 0 \text{ or } 1, \\ \mathcal{Z}_2 \times \mathcal{Z}_{2^{e-2}} \times \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{if } e \geq 2. \end{cases}$$

We find a primitive element $a \bmod n$ by choosing primitive elements $a_0 \bmod 2^e$ (if $e \geq 2$) and $a_i \bmod q_i$ and solving the simultaneous congruences $a \equiv a_i \pmod{q_i}$, and if applicable $a \equiv a_0 \pmod{2^e}$.

Proof. All this follows from the chinese remainder theorem. $\diamond$

Exercise Derive a general formula for $\lambda(n)$.

A.5 The Jacobi Symbol

Consider the multiplicative group $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ for a module $n \geq 2$, and its squaring map

$$\mathbf{q}\colon \mathbb{M}_n \longrightarrow \mathbb{M}_n, \quad x \mapsto x^2 \bmod n\,.$$

$\mathbf{q}$ is a group homomorphism. The elements in the image of $\mathbf{q}$ are the **quadratic residues** mod n. An integer x is a quadratic residue mod n if $x \bmod n$ is invertible, and there exists an integer u with $u^2 \equiv x \pmod{n}$. Thus the set of quadratic residues is the subset $\mathbb{M}_n^2$ of the residue class ring $\mathbb{Z}/n\mathbb{Z}$. (This notation is not standard just as little as $\mathbb{M}_n$. But it spares writing $((\mathbb{Z}/n\mathbb{Z})^\times)^2$ over and over again.)

Remarks and Examples

1. For $n = 2$ we have $\mathbb{M}_n^2 = \mathbb{M}_n = \{1\}$.

2. For $n \geq 3$ we have $-1 \neq 1$ and $(-1)^2 = 1$. Hence $\mathbf{q}$ is not injective and thus also not surjective. Therefore quadratic non-residues exist.

3. Let $n = p \geq 3$ be prime. Then the kernel of $\mathbf{q}$ exactly consists of the zeroes of the polynomial $X^2 - 1$ in the field $\mathbb{F}_p$, hence of $\{\pm 1\}$. We conclude that the number of quadratic residues is $\frac{p-1}{2}$.

4. More generally let $n = q = p^e$ be a power of an odd prime p. Then $\mathbb{M}_n$ is cyclic of order $\varphi(q) = q \cdot (1 - \frac{1}{p})$ by Proposition 18. Thus 1 has exactly the square roots ± 1 in $\mathbb{M}_q$, and the number of quadratic residues is $\varphi(q)/2$.

5. Let n be a product of two different odd primes p and q. By the chinese remainder theorem the natural map $\mathbb{M}_n \longrightarrow \mathbb{M}_p \times \mathbb{M}_q$ is an isomorphism. Hence $\mathbb{M}_n$ contains exactly four square roots of 1, and $\mathbb{M}_n^2 \leq \mathbb{M}_n$ is a subgroup of index 4.

6. In the general case let $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition with different odd primes $p_1, \ldots, p_r$, and $r \geq 0$, $e \geq 0$, $e_1, \ldots, e_r \geq 1$. Proposition 2 tells us the number of square roots of 1 in $\mathbb{M}_n$:

$$\begin{array}{ll} 2^r, & \text{if } e = 0 \text{ or } 1, \\ 2^{r+1}, & \text{if } e = 2, \\ 2^{r+2}, & \text{if } e \geq 3. \end{array}$$

   This number is also the order of the kernel of $\mathbf{q}$, hence the index of $\mathbb{M}_n^2$ in $\mathbb{M}_n$.

The naive algorithm, exhaustion, for determing the quadratic residuosity of a mod n tries $1^2, 2^2, 3^2, \ldots$ until it hits a. A quadratic non-residue always takes $\lfloor \frac{n}{2} \rfloor$ steps, a quadratic residue $n/4$ steps in the average. Thus the costs grow exponentially with the number $\log n$ of places.

For the case where n is *prime* we'll see better algorithms.

The phenomen that there is no efficient algorithm for *composite* integers n is the basis of many cryptographic constructions, for instance the simplest perfect random generator (BBS, see Part IV).

For a prime module p the LEGENDRE **symbol** indicates quadratic residuosity:

$$(\frac{x}{p}) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue,} \\ 0 & \text{if } p|x, \\ -1 & \text{otherwise.} \end{cases}$$

The LEGENDRE symbol defines a homomorphism

$$(\frac{\bullet}{p}) : \mathbb{M}_p \longrightarrow \mathbb{M}_p/\mathbb{M}_p^2 \cong \{\pm 1\}.$$

In the special case $p = 2$

$$(\frac{x}{2}) = \begin{cases} 1 & \text{if } x \text{ is odd,} \\ 0 & \text{if } x \text{ is even.} \end{cases}$$

Proposition 19 (EULER's criterion) *Let p be an odd prime. then*

$$x^{\frac{p-1}{2}} \equiv (\frac{x}{p}) \pmod p \quad \textit{for all } x.$$

Proof. If $p|x$ both sides equal 0. Otherwise $(x^{\frac{p-1}{2}})^2 = x^{p-1} \equiv 1$, hence $x^{\frac{p-1}{2}} \equiv \pm 1$. Let a be primitive $\bmod p$. Then both sides equal -1, hence the assertion holds for $x = a$. Since both sides represent homomorphisms $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ the assertion is true for all powers of a, hence for all x that are no multiples of p. $\diamond$

EULER's criterion yields an efficient algorithm for deciding quadratic residuosity: We have to take $\frac{p-1}{2}$-th powers in $\mathbb{F}_p^\times$, and this costs at most $2\lfloor \log_2(\frac{p-1}{2}) \rfloor$ multiplications $\bmod p$. Taking the cost of modular multiplication into account we get an order of magnitude of $\log_2(p)^3$.

By EULER's criterion -1 is a quadratic residue if and only if $\frac{p-1}{2}$ is even, hence $p \equiv 1 \pmod 4$. The decision on 2 or 3 is significantly more difficult. However there is an even faster algorithm. It is the subject of the following Section A.6.

The LEGENDRE symbol has a natural generalization by the JACOBI symbol (that uses the same notation): For $n > 0$ with prime decomposition

$n = p_1 \cdots p_r$ (the p_i not necessarily distinct)

$$(\frac{x}{n}) := (\frac{x}{p_1}) \cdots (\frac{x}{p_r}) \quad \text{for } x \in \mathbb{M}_n.$$

In particular $(\frac{x}{n}) = 0$ if x and n are not coprime. The supplementing definitions $(\frac{x}{1}) = 1$, $(\frac{x}{n}) = (\frac{x}{-n})$ for $n < 0$, and $(\frac{x}{0}) = 0$, make the JACOBI symbol a function

$$(\frac{\bullet}{\bullet}) : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

with values in $\{0, \pm 1\}$, and multiplicative in numerator and denominator. In particular the JACOBI symbol defines a homomorphism $(\frac{\bullet}{n})$ from $\mathbb{M}_n$ to $\{\pm 1\}$. But it is *not* an indicator of quadratic residuosity. Denoting $\mathbb{M}_n^+ = \ker(\frac{\bullet}{n})$ and $\mathbb{M}_n^- = \mathbb{M}_n - \mathbb{M}_n^+$, in general $\mathbb{M}_n^2$ is a proper subgroup of $\mathbb{M}_n^+$. Its index is given by example 6 above: If the number of square roots of 1 is 2^k with $k \geq 1$, then $\mathbb{M}_n^2$ has index 2^{k-1} in $\mathbb{M}_n^+$.

In any case $(\frac{x}{n})$ depends on the residue class x mod n only. Obviously

$$(\frac{x}{2^k}) = \begin{cases} 1, & \text{if } x \text{ is odd,} \\ 0, & \text{if } x \text{ is even.} \end{cases}$$

A.6 Quadratic Reciprocity

Quadratic reciprocity provides a very convenient method of computing the JACOBI (or LEGENDRE) symbol and thereby deciding quadratic residuosity. It relies on the following two propositions and a lemma that helps to reduce composite modules to prime modules.

Lemma 15 *Let $s, t \in \mathbb{Z}$ be odd. Then*

(i) $\frac{s-1}{2} + \frac{t-1}{2} \equiv \frac{st-1}{2} \pmod 2$,

(ii) $\frac{s^2-1}{8} + \frac{t^2-1}{8} \equiv \frac{s^2t^2-1}{8} \pmod 2$.

Proof. Assume $s = 2k+1$ and $t = 2l+1$. Then $st = 4kl + 2k + 2l + 1$,

$$\frac{st-1}{2} = 2kl + k + l \;\equiv\; k + l = \frac{s-1}{2} + \frac{t-1}{2}.$$

Moreover

$$s^2 = 4\cdot(k^2+k)+1, \quad t^2 = 4\cdot(l^2+l)+1,$$
$$s^2t^2 = 16\cdot\ldots + 4\cdot(k^2+k+l^2+l)+1,$$
$$\frac{s^2t^2-1}{8} = 2\cdot\ldots + \frac{k^2+k+l^2+l}{2},$$

and this proves the assertion. $\diamond$

Proposition 20 *Let n be odd. Then*

(i) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$,

(ii) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

Proof. The lemma reduces the assertions to the case $n = p$ prime.

(i) is a direct consequence of EULER's criterion, Proposition 19.

(ii) We have

$$(-1)^k \cdot k \equiv \begin{cases} k, & \text{if } k \text{ is even,} \\ p-k, & \text{if } k \text{ is odd,} \end{cases}$$

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k \cdot k \equiv 2\cdot 4 \cdots (p-1) = 2^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})!.$$

Om the other hand

$$\prod_{k=1}^{\frac{p-1}{2}}(-1)^k \cdot k = (\frac{p-1}{2})! \cdot (-1)^{\frac{p^2-1}{8}}, \quad \text{since} \quad \sum_{k=1}^{\frac{p-1}{2}} k = \frac{(p-1)(p+1)}{2 \cdot 2 \cdot 2}.$$

Now $(\frac{p-1}{2})!$ is a product of positive integers $< p$, thus not a multiple of p. Hence we may divide by it. Then from the two equations and EULER's criterion we get

$$(-1)^{\frac{p^2-1}{8}} \equiv 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) \pmod p\,.$$

Since $p \geq 3$ this congruence implies equality. $\diamond$

In particular 2 is a quadratic residue modulo the prime p if and only if $(p^2-1)/8$ is even, or $p^2 \equiv 1 \pmod{16}$, or $p \equiv 1$ or $7 \pmod 8$.

Theorem 3 (Law of Quadratic Reciprocity) *Let m and n be two different odd coprime positive integers. Then*

$$(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Here is a somewhat more comprehensible formula:

$$(\frac{m}{n}) = \begin{cases} -(\frac{n}{m}) & \text{if } m \equiv n \equiv 3 \pmod 4, \\ (\frac{n}{m}) & \text{else.} \end{cases}$$

The proof is in the next section. First we illustrate the computation with an example:

Is 7 a quadratic residue mod 107? *No*, as the following computation shows:

$$(\frac{7}{107}) = -(\frac{107}{7}) = -(\frac{2}{7}) = -1.$$

Likewise 7 is not a quadratic residue mod 11:

$$(\frac{7}{11}) = -(\frac{11}{7}) = -(\frac{4}{7}) = -(\frac{2}{7})(\frac{2}{7}) = -1.$$

Hence 7 is a quadratic non-residue also mod $1177 = 11 \cdot 107$. But $(\frac{7}{1177}) = 1$.

From the law of quadratic reciprocity we derive the following algorithm:

Procedure JacobiSymbol

Input parameters:
m, n = two integers.
Output parameter:
jac $= (\frac{m}{n})$.
Instructions:
If $n = 0$ output jac $= 0$ **end**
If $m = 0$ output jac $= 0$ **end**
If $\gcd(m, n) > 1$ output jac $= 0$ **end**
[*Now $m, n \neq 0$ are coprime, so jac $= \pm 1$.*]
jac $= 1$.
If $n < 0$ replace n by $-n$.
If n is even divide n by the maximum possible power 2^k.
If $m < 0$
 replace m by $-m$,
 if $n \equiv 3 \pmod 4$ replace jac by $-$jac.
[*From now on m and n are coprime, and n is positive and odd.*]
[*In the last step $m = 0$ and $n = 1$ may occur.*]
If $m > n$ replace m by $m \bmod n$.
While $n > 1$:
 If m is even:
  Divide m by the maximum possible power 2^k,
  if (k is odd and $n \equiv \pm 3 \pmod 8$) replace jac by $-$jac.
 [*Now m and n are odd and coprime, $0 < m < n$.*]
 [*The law of quadratic reciprocity applies.*]
 If ($m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$)
  replace jac by $-$jac.
 Set $d = m$, $m = n \bmod m$, $n = d$.

The analysis of this algorithm resembles the analysis of the Euclidean algorithm: We need at most $5 \cdot \log(m)$ steps, each one essentially consisting of one integer division. Since the size of the operands rapidly decreases, the total cost amounts to $O(\log_2(m)^2)$. This is significantly faster than applying Euler's criterion.

A.7 Proof of the Law of Quadratic Reciprocity

Now for the proof of the law of quadratic reciprocity. In the literature we find many different proofs. We adapt one that uses the theory of finite fields and follows ideas by ZOLOTAREV (Nouvelles Annales de Mathematiques 11 (1872), 354–362) and SWAN (Pacific J. Math. 12 (1962), 1099–1106).

Lemma 16 *Let p an odd prime, and a and p be coprime. Then the following statements are equivalent:*

(i) *a is a quadratic residue* $\bmod p$.

(ii) *Multiplication by a is an even permutation of $\mathbb{F}_p$.*

Proof. Denote the multiplication by $\mu_a : \mathbb{F}_p \longrightarrow \mathbb{F}_p$, $x \mapsto ax \bmod p$. Then $a \mapsto \mu_a$ is an injective group homomorphism $\mu : \mathbb{F}_p^\times \longrightarrow \mathfrak{S}_p$ to the full permutation group on p elements. If a is primitive, then μ_a has exactly two cycles: $\{0\}$ and $\mathbb{F}_p^\times$. Since p is odd, the sign of μ_a is $\sigma(\mu_a) = (-1)^{p-2} = -1$, hence μ_a is an odd permutation.

Since a generates the group $\mathbb{F}_p^\times$, the two homomorphisms

$$\left(\frac{\bullet}{p}\right) \quad \text{and} \quad \sigma \circ \mu : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$$

must be identical, and this was the assertion. ◇

As another tool we use the **discriminant** of a polynomial $f = a_n T^n + \cdots + a_0 \in K[T]$. We can compute it in any extension field $L \supseteq K$ that contains all the zeroes $t_1, \ldots, t_n$ of f by the formula

$$D(f) = a_n^{2n-2} \cdot \prod_{1 \le i < j \le n} (t_i - t_j)^2.$$

> The discriminant is invariant under all permutations of the zeroes. Hence it is in K. In our case this will also follow from the explicit computation.

The ususal method of computing the discriminant from the coefficients consists in comparing it with the resultant of f and its derivative f'. For the cyclotomic polynomial $f = T^n - 1$ the computation is outstandingly simple:

Lemma 17 *Assume that* $\operatorname{char} K$ *doesn't divide n. Then the polynomial $f = T^n - 1 \in K[T]$ has discriminant*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot n^n.$$

Proof. Let ζ be a primitive n-th root of unity (in some suitable extension field). Then

$$\begin{aligned} f &= \prod_{i=0}^{n-1}(T-\zeta^i), \\ D(f) &= \prod_{0\le i<j\le n-1}(\zeta^i-\zeta^j)^2 = (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i\neq j}(\zeta^i-\zeta^j) \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i=0}^{n-1}\left[\zeta^i \cdot \prod_{k=1}^{n-1}(1-\zeta^k)\right]. \end{aligned}$$

The polynomial

$$g = T^{n-1} + \cdots + 1 = \prod_{k=1}^{n-1}(T-\zeta^k) \in K[T]$$

satisfies $g(1) = n$. Hence

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i=0}^{n-1}[\zeta^i \cdot n] = (-1)^{\frac{n(n-1)}{2}} \cdot n^n,$$

as claimed. $\diamond$

Lemma 18 *Let p be an odd prime and n an odd integer, coprime with p. Then the following statements are equivalent:*

(i) *The discriminant of $T^n - 1 \in \mathbb{F}_p[T]$ is a quadratic residue* $\bmod p$.

(ii) *$l = (-1)^{(n-1)/2} \cdot n$ is a quadratic residue* $\bmod p$.

Proof. By Lemma 17 the discriminant is $D(f) = l^n$. Let $n = 2k+1$. Then $D(f)$ is the product of l with the quadratic residue l^{2k}. $\diamond$

The discriminant of a polynomial $f \in K[T]$ is a square in an extension field $L \supseteq K$ that contains the zeroes of f:

$$D(f) = \Delta(f)^2 \quad \text{with} \quad \Delta(f) = a_n^{n-1} \cdot \prod_{i<j}(t_i - t_j).$$

But $\Delta(f)$ inherits the sign of a permutation of the zeroes. Thus is not invariant, and therefore in general is not contained in K.

Proof of the theorem. Because of Lemma 15 (i) it suffices to prove the quadratic reciprocity law for two different odd primes p and q.

Let $K = \mathbb{F}_p$, ζ be a primitive q-th root of unity, $L = K(\zeta)$, and $f = T^q - 1$. Then $\zeta \mapsto \zeta^p$ defines a permutation μ_p of the roots of unity, and an automorphism of L over K. Thus:

$$\sigma(\mu_p) \cdot \Delta(f) = \prod_{i<j} (\zeta^{pi} - \zeta^{pj}) = \Delta(f)^p.$$

This yields a chain of equivalent statements:

$$(-1)^{\frac{q-1}{2}} \cdot q \text{ quadratic residue } \bmod p \Longleftrightarrow D(f) \text{ quadratic residue } \bmod p$$

$$\Longleftrightarrow \Delta(f) \in \mathbb{F}_p \Longleftrightarrow \Delta(f) = \Delta(f)^p \Longleftrightarrow \sigma(\mu_p) = 1$$

$$\Longleftrightarrow p \text{ quadratic residue } \bmod q.$$

From Proposition 20 (i) we get

$$(\frac{p}{q}) = (\frac{(-1)^{\frac{q-1}{2}} q}{p}) = (\frac{q}{p}) \cdot (\frac{-1}{p})^{\frac{q-1}{2}} = (\frac{q}{p}) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

as claimed. $\diamondsuit$

A.8 Quadratic Non-Residues

How to find a quadratic *non-residue* modulo a prime p? That is, an integer a with $p \nmid a$ that is not a quadratic residue $\bmod a$. The preferred solution is the smallest possible positive one. Nevertheless we start with -1:

Proposition 21 *Let $p \geq 3$ be prime.*

(i) -1 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 3 \pmod 4$.

(ii) 2 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 3$ *or* $5 \pmod 8$.

(iii) *(For $p \geq 5$)* 3 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 5$ *or* $7 \pmod{12}$.

(iv) *(For $p \geq 7$)* 5 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 2$ *or* $3 \pmod 5$.

Proof. (i) This follows from Proposition 20. However there is an even simpler proof:

$$\begin{aligned} -1 \in \mathbb{M}_p^2 &\iff \bigvee_{i \in \mathbb{Z}} i^2 \equiv -1 \pmod p \iff \bigvee_{i \in \mathbb{Z}} \operatorname{ord}_p i = 4 \\ &\iff 4 \mid \# \mathbb{F}_p^\times = p-1 \iff p \equiv 1 \pmod 4. \end{aligned}$$

(ii) This also follows from Proposition 20: By the adjacent remark $2 \in \mathbb{M}_p^2 \iff p \equiv 1$ or $7 \pmod 8$.

(iii) We use the law of quadratic reciprocity:

$$\begin{aligned} (\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3}) &= \begin{cases} (-1)^{6k}(\frac{1}{3}) = 1 & \text{if } p = 12k+1, \\ (-1)^{6k+2}(\frac{2}{3}) = -1 & \text{if } p = 12k+5, \\ (-1)^{6k+3}(\frac{1}{3}) = -1 & \text{if } p = 12k+7, \\ (-1)^{6k+5}(\frac{2}{3}) = 1 & \text{if } p = 12k+11, \end{cases} \\ &= \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12}, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases} \end{aligned}$$

(iv) By quadratic reciprocity

$$(\frac{5}{p}) = (\frac{p}{5}) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod 5, \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod 5, \end{cases}$$

as claimed. ◇

Corollary 1 241 *is the unique odd prime* < 400 *for which none of* -1, 2, 3, 5 *are quadratic non-residues.*

Corollary 2 *For each odd prime p at least one of -1, 2, 3, or 5 is a quadratic non-residue except for $p \equiv 1, 49 \pmod{120}$.*

For arbitrary, not necessarily prime, modules we have some analogous results:

Lemma 19 *Let $n \in \mathbb{N}$, $n \geq 2$. Assume that $(\frac{a}{n}) = -1$ for some $a \in \mathbb{Z}$. Then a is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition. Then

$$(\frac{a}{n}) = (\frac{a}{p_1})^{e_1} \cdots (\frac{a}{p_r})^{e_r}.$$

Hence for some k the exponent e_k is odd, and $(\frac{a}{p_k}) = -1$. Then a is a quadratic non-residue mod p_k. Since $\mathbb{F}_{p_k}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$, a is a forteriori a quadratic non-residue mod n. $\diamond$

Corollary 3 *Let $n \in \mathbb{N}$, $n \geq 2$, and not a square in $\mathbb{Z}$.*

(i) *If $n \equiv 3 \pmod 4$, then -1 is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

(ii) *If $n \equiv 5 \pmod 8$, then 2 is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

And so on. Unfortunately this approach doesn't completely cover all cases, see the remark below. Nevertheless we note that an algorithm for finding a quadratic non-residue needs to address the cases $n \equiv 1 \pmod 8$ only. Again there are two variants:

- A deterministic algorithm that tests $a = 2, 3, 5, \ldots$ in order. Assuming ERH—for the character $\chi = (\frac{\bullet}{n})$—it is polynomial in the number $\log(n)$ of places.
- A probabilistic algorithm that randomly chooses a and succeeds with probability $\frac{1}{2}$ each time, yielding $(\frac{a}{n}) = -1$. Computing the Jacobi symbol takes $O(\log(n)^2)$ steps. In the average we need two trials to hit a quadratic non-residue.

Exercise For which prime modules is 7, 11, or 13 a quadratic non-residue? What is the smallest prime module for which this approach (together with Proposition 21) doesn't provide a quadratic non-residue?

Remark A result by Chowla/Fridlender/Salié says that (with a constant $c > 0$) there are infinitely many primes such that all integers a with $1 \leq a \leq c \cdot \log(p)$ are quadratic residues mod p. Ringrose/Graham and—assuming ERH—Montgomery have somewhat stronger versions of this result.

Remark There is no global polynomial (in $\log(n)$) upper bound for the smallest quadratic non-residue that is valid for all modules n. A very weak but simple result is in the following proposition.

Proposition 22 *Let $p \geq 3$ be a prime. Then there is a quadratic non-residue $a < 1 + \sqrt{p}$.*

Proof. There are quadratic non-residues > 1 (and $< p$). Let a be the smallest of these. Let $m = \lceil \frac{p}{a} \rceil$. Thus $(m-1) \cdot a < p < m \cdot a$, or

$$0 < m \cdot a - p < a.$$

Hence $m \cdot a \equiv m \cdot a - p$ is a quadratic residue. This is possible only if m is a quadratic non-residue. Since a is minimal we have $a \leq m$. We conclude

$$(a-1)^2 < (m-1) \cdot a < p,$$

hence $a - 1 < \sqrt{p}$. ◇

Relevant references

- V. R. Fridlender: On the least n-th power non-residue. Dokl. Akad. Nauk. SSSR 66 (1949), 351–352.
- H. Salié: Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl. Math. Nachr. 3 (1949), 7–8.
- N. C. Ankeney: The least quadratic nonresidue. Ann. of Math. 55 (1952), 65–72.
- H. L. Montgomery: *Topics in Multiplicative Number Theory.* Springer LNM 227 (1971).
- J. Buchmann/V. Shoup: Constructing nonresidues in finite fields and the extended Riemann hypothesis. Preprint 1990.
- S. W. Graham/C. Ringrose: Lower bounds for least quadratic non-residues. In: B. C. Berndt et al. (Eds): *Analytic Number Theory,* Birkhäuser, Boston 1990, 270–309.
- D. J. Bernstein: Faster algorithms to find non-squares modulo worst-case integers. Preprint 2002.

A.9 Primitive Elements for Special Primes

For many prime modules finding quadratic non-residues has turned out to be extremely easy. The same is true for finding primitive roots.

Proposition 23 *Let $p = 2p' + 1$ be a special prime. Then:*

(i) $a \in [2 \ldots p-2]$ *is a primitive root* mod p *if and only if it is a quadratic non-residue.*

(ii) $(-1)^{\frac{p'-1}{2}} \cdot 2$ *is a primitive root* mod p.

Proof. We have $p \equiv 3 \pmod 4$, thus -1 is a quadratic non-residue by Proposition 21.

(i) Since the order $\#\mathbb{F}_p^\times = p - 1$ is even, moreover each primitive root is also a quadratic non-residue. There are $\varphi(p-1) = p' - 1$ of them, thus we have found p' quadratic non-residues. Since $p' = \frac{p-1}{2}$, these must be all of them.

(ii) In the case $p' \equiv 1 \pmod 4$ we have $p \equiv 3 \pmod 8$, hence $2 = (-1)^{\frac{p'-1}{2}} \cdot 2$ is a quadratic non-residue by Proposition 21, hence also primitive.

In the case $p' \equiv 3 \pmod 4$ we have $p \equiv 7 \pmod 8$, hence 2 is a quadratic residue, and -1 is a quadratic non-residue again by Proposition 21. Therefore $-2 = (-1)^{\frac{p'-1}{2}} \cdot 2$ is a quadratic non-residue, hence also primitive. ◇

The effortlessness of finding a primitive root is one of several reasons why cryptologists like special primes.

Corollary 1 *Let $p = 2p' + 1$ be a special prime. Then the order of* 2 *in* $\mathbb{F}_p^\times$ *is*

(i) $p - 1 = 2p'$ *if* $p' \equiv 1 \pmod 4$,

(ii) $(p-1)/2 = p'$ *if* $p' \equiv 3 \pmod 4$.

Proof. (i) 2 is a primitive root.

(ii) The divisors of $\#\mathbb{F}_p^\times$ are $\{1, 2, p', 2p'\}$. Since 2 is a quadratic residue, it is not primitive, hence the order is not $2p'$. The order cannot be 1 since $2 \neq 1$ in $\mathbb{F}_p$. And the order 3 would imply that $4 = 1$, hence $3 = 0$ in $\mathbb{F}_p$, hence $p = 3$ which ic not a special prime. ◇

A.10 Some Group Theoretic Trivia

Here we collect some elementary results on finite groups. The exponent of a group G is the minimum positive integer e (or ∞) such that $x^e = \mathbf{1}$ for all $x \in G$. Denote the order of a group element x by $\operatorname{ord} x$ (positive integer or ∞).

Lemma 20 *Let G be a finite group with exponent e. Then $e \mid \#G$, and $e = t := \operatorname{lcm}(\{\operatorname{ord} x \mid x \in G\})$.*

Proof. By LAGRANGE's Theorem $\operatorname{ord} x \mid \#G$ for all $x \in G$, hence $e \mid \#G$. Moreover $x^e = \mathbf{1}$ by definition of e, hence $\operatorname{ord} x \mid e$ for all $x \in G$. Hence $t \mid e$. Sinc $x^t = \mathbf{1}$ for all x, even $t = e$. $\diamond$

Lemma 21 *Let G and H be groups, $g \in G$ with $\operatorname{ord} g = r$ and $h \in H$ with $\operatorname{ord} h = s$. Then $\operatorname{ord}(g, h) = \operatorname{lcm}(r, s)$ in the direct product $G \times H$.*

Proof.

$$(g^e, h^e) = (g, h)^e = \mathbf{1} \text{ in } G \times H \iff g^e = \mathbf{1} \text{ in } G \text{ and } h^e = \mathbf{1} \text{ in } H.$$

$\diamond$

Lemma 22 *Let G be a group with exponent r and H be a group with exponent s. Then the direct product $G \times H$ has exponent $t := \operatorname{lcm}(r, s)$.*

Proof. Since $r, s \mid t$ we have $(g, h)^t = (g^t, h^t) = (\mathbf{1}, \mathbf{1})$ for all $g \in G$ and $h \in H$. Thus the exponent e of $G \times H$ is $\leq t$.

Since $(\mathbf{1}, \mathbf{1}) = (g, h)^e = (g^e, h^e)$ for all g, h, we have $r \mid e$ and $s \mid e$, hence $t \mid e$. $\diamond$

Lemma 23 *Let G be a cyclic group of prime order r, and H, a cyclic group of prime order $s \neq r$. Then the direct product $G \times H$ is cyclic of order $r \cdot s$.*

Proof. Let $g \in G$ have order r, and $h \in H$ have order s. Then by Lemma 21 the element (g, h) has order $\operatorname{lcm}(r, s) = r \cdot s = \#(G \times H)$, hence generates $G \times H$. $\diamond$

Lemma 24 *Let G be an abelian group.*

(i) *Let $a, b \in G$, $\operatorname{ord} a = r$, $\operatorname{ord} b = s$, where r, s are finite and coprime. Then $\operatorname{ord}(ab) = rs$.*

(ii) *Let* $a, b \in G$, $\operatorname{ord} a = r$ *and* $\operatorname{ord} b = s$ *finite,* $t := \operatorname{lcm}(r, s)$. *Then* $\operatorname{ord}(ab) \mid t$, *and there is a* $c \in G$ *with* $\operatorname{ord} c = t$.

(iii) *Let* $m = \max\{\operatorname{ord} a \mid a \in G\}$ *be finite. Then* $\operatorname{ord} b \mid m$ *for all* $b \in G$. *In particular* m *is the exponent of* G.

Proof. (i) Let $k := \operatorname{ord}(ab)$. From $(ab)^{rs} = (a^r)^s \cdot (b^s)^r = \mathbf{1}$ we conclude that $k \mid rs$. Conversely, since $a^{ks} = a^{ks} \cdot (b^s)^k = (ab)^{ks} = \mathbf{1}$ we have $r \mid ks$, hence $r \mid k$, and likewise $s \mid k$, hence $rs \mid k$.

(ii) Let $k := \operatorname{ord}(ab)$. From $(ab)^t = a^t \cdot b^t = \mathbf{1}$ follows that $k \mid t$.

Now let p^e be a prime power with $p^e \mid t$, say $p^e \mid r$. Then a^{r/p^e} has order p^e. Let $t = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition with different primes p_i. Then there are $c_i \in G$ with $\operatorname{ord} c_i = p_i^{e_i}$. Since these orders are pairwise coprime, the element $c = c_1 \cdots c_r$ has order t by (i).

(iii) Let $\operatorname{ord} b = s$. Then by (ii) there is a $c \in G$ with $\operatorname{ord} c = \operatorname{lcm}(m, s)$. Hence $\operatorname{lcm}(m, s) \leq m$, hence $= m$, thus $s \mid m$. ◇

Remarks

1. For non-abelian groups all three statements (i)–(iii) may be false. As an example consider the symmetric group $\mathcal{S}_4$ of order $4! = 24$. The possible orders of its elements are 1 (for the trivial permutation), 2 for permutations consisting of one or two disjoint 2-cycles, 3 for all 3-cycles, and 4 for all 4-cycles. Thus the maximum order is 4, but the exponent = the lcm of all orders is 12 (by Lemma 20). The cycle $\sigma = (1\,2\,3)$ has order $r = 3$, the transposition $\tau = (3\,4)$ has order $s = 2$. Their product is the 4-cycle $(2\,3\,4\,1)$ of order $4 \neq \operatorname{lcm}(r, s) = 6$, and there doesn't exist any permutation of order 6.

2. In a nontrivial abelian group the order of a product ab in general differs from the lcm of the single orders: Take $a \neq \mathbf{1}$ and $b = a^{-1}$.

A.11 Blum Integers

Let $n = pq$ with different primes $p, q \geq 3$. Then

$$\mathbb{M}_n \cong \mathbb{M}_p \times \mathbb{M}_q, \quad \mathbb{M}_n^2 \cong \mathbb{M}_p^2 \times \mathbb{M}_q^2,$$

$$\mathbb{M}_n/\mathbb{M}_n^2 \cong \mathbb{M}_p/\mathbb{M}_p^2 \times \mathbb{M}_q/\mathbb{M}_q^2 \cong \mathcal{Z}_2 \times \mathcal{Z}_2,$$

in particular $\#(\mathbb{M}_n/\mathbb{M}_n^2) = 4$. The subgroups $\mathbb{M}_n^2 \leq \mathbb{M}_n^+$ and $\mathbb{M}_n^+ \leq \mathbb{M}_n$ are proper and hence of index 2. The ring $\mathbb{Z}/n\mathbb{Z}$ contains exactly 4 roots of unity: $1, -1, \tau, -\tau$, where

$$\tau \equiv -1 \pmod p, \quad \tau \equiv 1 \pmod q,$$

thus $(\frac{\tau}{n}) = -1$. In other words: The kernel of the squaring homomorphism $\mathbf{q} : \mathbb{M}_n \longrightarrow \mathbb{M}_n^2$ is $K = \{\pm 1, \pm \tau\}$, isomorphic with the Klein four-group.

An integer of the form $n = pq$ with different primes $p, q \equiv 3 \pmod 4$ is called Blum **integer**.

Examples

1. 1177 in A.6.
2. If p is a special prime, then $p \equiv 3 \pmod 4$. Therefore a product of two special primes is a Blum integer. Let us call such an integer a **special** Blum **integer**.

In general, if $n = pq$ with different odd prime numbers p and q, then $\mathbb{M}_n^2 \cong \mathbb{M}_p^2 \times \mathbb{M}_q^2$ has order $\frac{p-1}{2} \cdot \frac{q-1}{2}$, and this number is odd if and only if p and q both are $\equiv 3 \pmod 4$. Hence:

Lemma 25 *A product n of two odd prime numbers is a* Blum *integer if and only if the group $\mathbb{M}_n^2$ of quadratic residues has odd order.*

For a Blum integer -1 is a quadratic non-residue in $\mathbb{M}_p$ and $\mathbb{M}_q$, hence also in $\mathbb{M}_n$. But

$$(\frac{-1}{n}) = (\frac{-1}{p})(\frac{-1}{q}) = (-1)^2 = 1,$$

thus $-1 \in \mathbb{M}_n^+$. Hence

$$(\frac{-x}{n}) = (\frac{-1}{n})(\frac{x}{n}) = (\frac{x}{n})$$

for all x. Moreover $\mathbb{M}_n^2 \cap K = \{1\}$, thus the restriction of $\mathbf{q}$ to $\mathbb{M}_n^2$ is injective, hence bijective, and $\mathbb{M}_n$ is the direct product

$$\mathbb{M}_n = K \times \mathbb{M}_n^2, \quad \mathbb{M}_n^+ = \{\pm 1\} \times \mathbb{M}_n^2.$$

Each quadratic residue $a \in \mathbb{M}_n^2$ has exactly one square root in each of the four cosets of $\mathbb{M}_n/\mathbb{M}_n^2$. If $x \in \mathbb{M}_n^2$ is one of them, then the other ones are $-x$, τx, $-\tau x$. This shows:

Proposition 24 *Let n be a* Blum *integer. Then:*

(i) *If $x^2 \equiv y^2 \pmod{n}$ for $x, y \in \mathbb{M}_n$, and $x, -x, y, -y \bmod n$ are pairwise distinct, then $(\frac{x}{n}) = -(\frac{y}{n})$.*

(ii) *The squaring homorphism $\mathbf{q}$ is an automorphism of $\mathbb{M}_n^2$.*

(iii) *Each $a \in \mathbb{M}_n^2$ has has exactly two square roots in $\mathbb{M}_n^+$. If x is one of them, then $-x \bmod n$ is the other one, and exactly one of these two is itself a quadratic residue. Moreover a has exactly two more square roots, and these are contained in $\mathbb{M}_n^-$.*

Thus from the four square roots of a quadratic residue x exactly one is itself a quadratic residue. We consider this one as something special, and denote it by $\sqrt{x} \bmod n$. The least significant bit of x—also characterized as the parity of x, or as $x \bmod 2$—is denoted by $\operatorname{lsb}(x)$.

Corollary 1 *Let $x \in \mathbb{M}_n^+$. Then x is a quadratic residue if and only if*

$$\operatorname{lsb}(x) = \operatorname{lsb}(\sqrt{x^2} \bmod n).$$

Proof. If x is a quadratic residue, then $x = \sqrt{x^2} \bmod n$. Now assume x is a quadratic non-residue, and let $y = \sqrt{x^2} \bmod n$. By (iii) we have $y = -x \bmod n = n - x$. Since n is odd, x and y have different parities. $\diamond$

The problem of deciding quadratic residuosity $\bmod n$ remains hard. Only if the prime decomposition $n = pq$ is known there is an efficient solution:

$$x \in \mathbb{M}_n^2 \iff (\frac{x}{p}) = (\frac{x}{q}) = 1.$$

We know of no efficient procedure that works without using the prime factors. *Presumably* deciding quadratic residuosity is equivalent with factoring in the sense of complexity theory. Generally believed to be true is the

Quadratic Residuosity Assumption: Deciding quadratic residuosity for Blum integers is hard.

A mathematical sound definition of "hard" is in Section B.7.

A.12 The Multiplicative Group Modulo Special Blum Integers

Let $p = 2p' + 1$ be a special prime. Then the multiplicative group $\mathbb{M}_p = \mathbb{F}_p^\times$ is cyclic of order $p - 1 = 2p'$. Its subgroup $\mathbb{M}_p^2 \leq \mathbb{M}_p$ of quadratic residues has index 2 and is itself cyclic, its order being the prime p'. Thus

$$\begin{aligned} \mathbb{M}_p &\cong \mathcal{Z}_{2p'}, \qquad & \#\mathbb{M}_p &= \varphi(p) = \lambda(p) = 2p', \\ \mathbb{M}_p^2 &\cong \mathcal{Z}_{p'}, \qquad & \#\mathbb{M}_p^2 &= p'. \end{aligned}$$

Let $n = pq$ be a special Blum integer, $p = 2p' + 1$ and $q = 2q' + 1$ being special primes. Then we know that

$$\begin{aligned} \mathbb{M}_n &\cong \mathbb{M}_p \times \mathbb{M}_q, \qquad & \#\mathbb{M}_n &= \varphi(n) = 4p'q', \\ \mathbb{M}_n^2 &\cong \mathbb{M}_p^2 \times \mathbb{M}_q^2, \qquad & \#\mathbb{M}_n^2 &= p'q'. \end{aligned}$$

Moreover $\lambda(n) = \mathrm{lcm}(2p', 2q') = 2p'q'$. Since $\mathbb{M}_n^2$ as a direct product of two cyclic groups of coprime orders is itself cyclic of order $p'q'$ we conclude:

Proposition 25 *Let n be a special* Blum *integer as above. Then the group $\mathbb{M}_n^2$ of quadratic residues* $\bmod n$ *is cyclic of order $p'q'$ and consists of*

(i) 1 *element of order* 1,

(ii) $p' - 1$ *elements x of order p', characterized by* $x \bmod q = 1$,

(iii) $q' - 1$ *elements x of order q', characterized by* $x \bmod p = 1$,

(iv) $(p' - 1)(q' - 1)$ *elements of order $p'q'$.*

Note that these numbers sum up to $p'q'$, the order of $\mathbb{M}_n^2$.

Corollary 1 *Let n be a special* Blum *integer with prime factors $p = 2p' + 1$ and $q = 2q' + 1$. Then the probability $\eta = P\{x \in \mathbb{M}_n^2 \mid \mathrm{ord}(x) = p'q'\}$ that a randomly chosen quadratic residue* $\bmod n$ *has the maximum possible order $p'q'$ is*

$$\eta = 1 - \frac{p' + q' - 1}{p'q'}.$$

If we follow the common usage of choosing (RSA or) BBS modules n as products of two l-bit primes, or p' and q' as $(l-1)$-bit primes, then

$$2^{l-1} < p' < 2^l, \quad 2^{l-1} < q' < 2^l,$$

$$2^l < p' + q' - 1 < 2^{l+1}, \quad 2^{2l-1} < p' \cdot q' < 2^{2l},$$

$$\frac{1}{2^l} = \frac{2^l}{2^{2l}} < \frac{p' + q' - 1}{p'q'} < \frac{2^{l+1}}{2^{2l-1}} = \frac{1}{2^{2l-3}} = \frac{8}{2^l}.$$

We resume

Corollary 2 *Let n be a special* BLUM *integer with prime factors $p = 2p' + 1$ and $q = 2q' + 1$ of bitlengths l. Then the probability η is bounded by*

$$1 - \frac{8}{2^l} \;<\; \eta \;<\; 1 - \frac{1}{2^l}.$$

The deviation of this probability from 1 is asymptotically negligible: If we choose a random quadratic residue x (say as the square of a random element of $\mathbb{M}_n$), then with overwhelming probability its order has the maximum possible value. However there is an easy test: Check that neither $x \bmod p$ nor $x \bmod q$ is 1.

Since $\mathbb{M}_n$ is the direct product of $\mathbb{M}_n^2$ with a KLEIN four-group we also know the orders of the elements of $\mathbb{M}_n$ and their numbers, in particular

Corollary 3 *Let n be a special* BLUM *integer with prime factors $p = 2p' + 1$ and $q = 2q' + 1$. Then $\mathbb{M}_n$ has exactly $(p' - 1)(q' - 1)$ elements of order $p'q'$, and exactly $3(p' - 1)(q' - 1)$ elements of order $2p'q'$.*

A.13 The BBS Sequence

Let n be a positive integer. Let x be invertible $\bmod n$, and let $s := \mathrm{ord}(x)$ be its order in the multiplicative group $\bmod n$.

Lemma 26 *For each integer r we have*

$$r \equiv 1 \pmod{s} \Longleftrightarrow x^r \equiv x \pmod{n}.$$

Proof. "$\Longrightarrow$": Let $r = 1 + c \cdot s$. Then

$$x^r = x^{1+c\cdot s} \equiv x \cdot 1 = x \bmod n.$$

"$\Longleftarrow$": Dividing $\bmod n$ by the invertible element x gives

$$x^{r-1} \equiv 1 \pmod{n},$$

hence $s \mid r - 1$. $\diamond$

Now let $x_0 := x$, and define the **BBS sequence** of integers x_i by the recursive formula $x_i = x_{i-1}^2$ for $i \geq 1$, or

$$x_i = x^{2^i} \bmod n \quad \text{for } i = 0, 1, 2, 3, \ldots \tag{1}$$

Lemma 27 *The BBS sequence (x_i) is purely periodic if and only if $s = \mathrm{ord}(x)$ is odd. Then the period ν equals the multiplicative order of $2 \bmod s$.*

Proof. Assume the sequence is purely periodic with period ν. Then ν is minimal with $x_\nu \equiv x_0 \pmod{n}$. Hence

$$x_0^{2^\nu} \equiv x_0 \pmod{n}.$$

Thus $s \mid (2^\nu - 1)$ by Lemma 26, and ν is minimal with this property too, or with $2^\nu \equiv 1 \bmod s$. In particular s is odd, and ν is the order of $2 \bmod s$.

Conversely assume that s is odd. Then 2 is invertible $\bmod s$. Let μ be the multiplicative order of $2 \bmod s$. Then $2^\mu \equiv 1 \bmod s$, hence $x_\mu = x^{2^\mu} \equiv x_0 \bmod n$ by Lemma 26, thus the sequence is purely periodic. $\diamond$

Proposition 26 *Let n be a* Blum *integer and x be a quadratic residue $\neq 1 \bmod n$. Then the BBS sequence x_i as defined in (1) is purely periodic of period $\nu = \mathrm{ord}_s(2)$.*

Proof. Assume $n = pq$ where p and q are two different odd primes $\equiv 3 \bmod 4$. Let $p = 4k+3$ and $q = 4l+3$ with integers k and l. Then the multiplicative group $\mathbb{M}_n$ has order $(p-1)(q-1) = (4k+2)(4l+2)$. The group $\mathbb{M}_n^2$ of quadratic residues has index 4 in $\mathbb{M}_n$, hence order $(2k+1)(2l+1)$, an odd integer. Thus every quadratic residue has odd order, and Lemma 27 applies for x. $\diamond$

Corollary 4 *Let n be a* Blum *integer and ν, the period of a BBS sequence. Then $\nu \mid \lambda(\lambda(n))$ where λ is the* Carmichael *function.*

Proof. By Proposition 26 we have $\nu = \mathrm{ord}_s(2) \mid \lambda(s)$. Moreover $s = \mathrm{ord}_n(x) \mid \lambda(n)$, hence $\lambda(s) \mid \lambda(\lambda(n))$. We conclude that $\nu \mid \lambda(\lambda(n))$. $\diamond$

A.14 The BBS Sequence for Superspecial Blum Integers

Again we get the most satisfying results in the superspecial case:

Definition A **superspecial** Blum **integer** is a product of two different superspecial primes.

Examples The two smallest superspecial primes are $p = 23$ (with $p' = 11$, $p'' = 5$) and $q = 47$ (with $q' = 23$, $q'' = 11$). Thus the smallest superspecial Blum integer is $n = 23 \cdot 47 = 1081$. By Section 2.1 we are confident (however don't know for sure) that there are very many superspecial Blum integers.

Now let $n = pq$ be a superspecial Blum integer with $p = 2p'+1 = 4p''+3$ and $q = 2q' + 1 = 4q'' + 3$. Form the BBS sequence (1) for an initial value $x \in \mathbb{M}_n^2 - \{1\}$. Then $s = \mathrm{ord}_n(x)$ takes one of the values p', q', or $p'q'$, the last on with extremely high probability, and the first two may be excluded by an easy check. The period of the BBS sequence is $\nu = \mathrm{ord}_s(2)$ by Proposition 26, and we may assume that $s = p'q'$. By the chinese remainder theorem and Lemma 21

$$\nu = \mathrm{lcm}(\mathrm{ord}_{p'}(2), \mathrm{ord}_{q'}(2))$$

By the Corollary of Proposition 23 in Section A.9

$$\mathrm{ord}_{p'}(2) = \begin{cases} 2p'' & \text{if } p'' \equiv 1 \pmod 4), \\ p'' & \text{if } p'' \equiv 3 \pmod 4), \end{cases}$$

$$\mathrm{ord}_{q'}(2) = \begin{cases} 2q'' & \text{if } q'' \equiv 1 \pmod 4), \\ q'' & \text{if } q'' \equiv 3 \pmod 4), \end{cases}$$

Thus finally we have shown:

Proposition 27 *Let n be a superspecial* Blum *integer. Let x be a quadratic residue* mod n *with $x \not\equiv 1 \pmod p$ and $x \not\equiv 1 \pmod q$. Then the BBS sequence* mod n *for x has period*

$$\nu = \begin{cases} p''q'' & \text{if } p'' \equiv q'' \equiv 3 \pmod 4, \\ 2p''q'' & \text{otherwise.} \end{cases}$$

If p'' and q'' are $(l-2)$-bit primes (hence $> 2^{l-3}$, and n is an l-bit integer), then the period is $> 2^{l-2}$ or about $n/4$.