Finite fields have cyclic multiplicative
groups &
NumThy: Primitive Roots : Algebra

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
31 July, 2018 (at 11:10)

Common notation. Use PoT for “power of two”; the
PoTs are 1, 2, 4, . . .

Use \( \equiv_N \) to mean “congruent mod \( N \)”. Let \( n \perp k \) mean
that \( n \) and \( k \) are co-prime. Use \( k \divides n \) for “\( \frac{n}{k} \) divides \( n \)”. Its
negation \( k \nmid n \) means “\( k \) does not divide \( n \).” Use \( n \bullet k \) and
\( n \nmid k \) for “\( n \) is/is-not a multiple of \( k \).” Finally, for \( p \) a prime
and \( E \) a natnum: Use double-vertices, \( p^E \bullet\nmid n \), to mean that \( E \)
is the highest power of \( p \) which divides \( n \). Or write \( n \bullet p^E \)
to emphasize that this is an assertion about \( n \). Use PoT for
Power of Two and PoP for Power of (a) Prime.

For \( N \) a posint, use \( \Phi(N) \) or \( \Phi_N \) for the set
\( \{r \in \{1\ldots N\} \mid r \perp N\} \). The cardinality \( \varphi(N) := |\Phi_N| \) is the Euler phi function. [So \( \varphi(N) \) is the cardinality of the multiplicative
group, \( \Phi_N \), in the \( \mathbb{Z}_N \) ring.] Easily, \( \varphi(p^r) = [p^r]-p^{r-1} \), for
prime \( p \) and posint \( L \).

Use EFT for the Euler-Form Thm, which says: Suppose
that integers \( b \perp L \), with \( L \) positive. Then \( b^{\varphi(L)} \equiv 1 \).

Bézout’s thm says: Given a finite list of integers, not all
zero, their GCD is some integer linear combination of the given integers.

Defn: The order of an element. Suppose \((S, \cdot)\) is a
semigroup [written multiplicatively, with unit] which is not
necessarily abelian, nor finite. Fix a \( y \in S \). A posint
\( n \) is “a period of \( y \)” if \( y^n = 1 \). Let

\[
\text{Per}_S(y) := \{ n \in \mathbb{Z}_+ \mid y^n = 1 \}.
\]

Written \( \text{Ord}_S(y) \) or just \( \text{Ord}(y) \), the order of \( y \) in
( semigroup \( S \) ) is the infimum of the periods of \( y \); so if
\( y \) has no periods [i.e \( y^n \) is never 1] then \( \text{Ord}(y) = \infty \).

Of course, when \( y \) has finite order, \( n \), then \( y \) is
invertible, since \( y \cdot y^{-1} = 1 \). Thus a semigroup in
which every element has finite order is automatically
a group. Consequently, assertions which would gain
no generality if stated for a semigroup \( S \), are stated
for a group \( G \).

Integers mod \( N \)

An integer \( y \) has a mod-\( N \) multiplicative-order IFF
\( y \perp N \). Let \( \text{Ord}(y) := \text{Ord}_N(y) \) denote this order,
and \( \text{Per}_N(y) \) the set of periods.

1: Prop’n. Suppose posints \( K \bullet N \) and \( y \perp N \). Then
\( \text{Ord}_K(y) \bullet \text{Ord}_N(y) \).

Proof. Let \( k := \text{Ord}_K(y) \). Bézout’s thm implies that
\( \text{Per}_K(y) \) equals \( k \mathbb{Z} \). For an \( n \in \text{Per}_N(y) \), note,
\( [y^n - 1] \bullet N \bullet K \). So \( n \in k \mathbb{Z} \).

Given a ring-hom \( h: \Gamma \to \Gamma’ \), easily the foward image
of the units \( h(U) \subset U’ \), where \( U, U’ \) are the respective
units-groups. Some units in \( U’ \) may be missed. E.g,
\( h: \mathbb{Z} \to \mathbb{Z}_5 \) by \( x \mapsto \langle x \rangle_5 \).

2: Prop’n. Fix posints \( N \bullet K \). Let \( h: \mathbb{Z}_N \to \mathbb{Z}_K \) be
the surjective ring-hom \( x \mapsto \langle x \rangle_K \). Then the \( h \)-image
of mult-group \( \Phi(N) \) is all of \( \Phi(K) \). In particular

\[ \Phi(N) \text{ cyclic } \Rightarrow \Phi(K) \text{ cyclic.} \]

Hence, if \( g \) is an \( N \)-primroot, then \( \langle g \rangle_K \) is a \( K \)-primroot.

Proof. Let \( Q := \frac{N}{K} \). Take the special case that \( K \perp Q \).
Then the CRTThm gives a ring-iso \( f: \mathbb{Z}_N \to \mathbb{Z}_K \times \mathbb{Z}_Q \) by
\( x \mapsto \langle \langle x \rangle_K, \langle x \rangle_Q \rangle \). Exercise: The set of units in
\( \mathbb{Z}_K \times \mathbb{Z}_Q \) is \( \Phi(K) \times \Phi(Q) \). Hence, for \( y \in \Phi(K) \): The
set \( h^{-1}(y) \) has precisely \( \varphi(Q) \)-many preimages which are
\( \mathbb{Z}_N \)-units, and \( Q - \varphi(Q) \) which are zero-divisors.

General case. Alas, \( K \) need not be co-prime to \( \frac{N}{K} \). So let \( \mathbb{K} \) be the product, over those primes
\( p \bullet K \), of \( p^{\varphi(p)} \), where \( p^{\varphi(p)} \bullet N \). Evidently \( \mathbb{K} \perp N/\mathbb{K} \).

A \( K \)-unit \( y \) evidently has \( y \perp \mathbb{K} \). By the above
special case, \( y \) has a “\( \mathbb{K} \)-lift” \( y + t\mathbb{K} \) which is co-prime
to \( N \). And it is also a \( K \)-lift, since \( K \bullet \mathbb{K} \).

Fields

Let \( F \) be a field, and let \( G \) be its multiplicative subgroup;
that is, \( G := F - \{0\} \). Fix \( n \) and consider all elements in \( F \) of period \( n \).
These are the roots of polynomial \( x^n - 1 \). A standard result about fields (see
“Integral domain question”, below) is that a polynomial of
degree $n$ can have at most $n$ roots. Thus the multiplicative group of the field is order-constrained: Say that a semigroup $S$ is order-constrained if,

3: For each positive integer $n$, there are at most $n$ elements $x \in S$ satisfying $x^n = 1$.

Our goal is to prove this theorem.

4: Field-Cyclic Theorem. Consider $F$, a finite field with $G := F \setminus \{0\}$ its multiplicative subgroup. Let $L := |G|$. Then $G$ is cyclic, that is, $(G, \cdot, 1)$ is group-isomorphic to $(\mathbb{Z}_L, +, 0)$.

The above theorem is an immediate corollary of the following, for which we will give two proofs.

5: Cyclic Theorem. Suppose $G$ is a finite group (possibly non-abelian) which is order-constrained. Then $G$ is cyclic.

Left to the reader is the easy converse:

5′: If $G$ is a finite cyclic group then $G$ is order-constrained.

Our first proof of (5) will work in general. The second proof only works for $G$ abelian; however, it proceeds via the LCM Lemma, which is interesting in its own right, and which applies even to infinite semigroups.

Proof of (5). Let $L := |G|$. Our goal is to show that there is an element of order $L$.

Counting elements in $G$. For each postive $m$ dividing $L$, let $\psi(m) = \psi_G(m)$ denote the number of elements of $G$ whose order is precisely $m$. Thus

5a: \[ \sum_{m \mid L} \psi(m) = |G| = L. \]

Now consider an $m$ for which $\psi(m)$ is not zero; so there is an element $b \in G$ whose order is $m$. This $b$ generates a copy of $(\mathbb{Z}_m, +, 0)$ inside of $G$, and this subgroup exhausts all the elements which are $m$-periodic, since $G$ is order-constrained. Hence the only elements of order $m$ are those in this copy of $\mathbb{Z}_m$; and there are $\varphi(m)$ of them.

The upshot: Each $\psi(m)$ is either 0 or is $\varphi(m)$. In particular

5b: For each $m$: $\psi_G(m) \leq \varphi(m)$.

Counting elements in $\mathbb{Z}_L$. Let’s apply the same analysis to $(\mathbb{Z}_L, +)$, which is order-constrained. For this group, we know that whenever $m$ divides $L$ there indeed is an element of order $m$; namely, the element $L/m$. So $\psi_{\mathbb{Z}_L}(m)$ always is $\varphi(m)$. Consequently, applying (5a) to $\mathbb{Z}_L$ provides that

5a′: \[ \sum_{m \mid L} \varphi(m) = |\mathbb{Z}_L| = L. \]

The two sums in (5a),(5a′) are equal. Yet (5b) provides a term-by-term inequality between the summands. Consequently, the summands must be equal term-by-term. In particular, $\psi_G(L) = \varphi(L)$, which is positive. So there are elements of order $L$ in $G$.

The second proof of (5), when $G$ is abelian

Our second proof proceeds via this lemma:

6: LCM Lemma. Suppose $S$ is an abelian semigroup, which may be infinite. For each two elements $a, b \in S$, the LCM of their orders, $\alpha$ and $\beta$, is itself the order of some element in sub-semigroup $(a, b) \subset S$.

In the $\alpha \perp \beta$ special-case, element $ab$ has order $\alpha \beta$.

Proof. WLOG both elements have finite order.

When $\alpha \perp \beta$. Write $\omega := \text{Ord}(ab)$. Since $[ab]^{\alpha \beta} = [a^{}][b^{}][a^{}] = 1 \cdot 1 = 1$, we have that $\omega \equiv \alpha \beta$. Thus ISTShow that $(\omega \cdot \alpha \beta)$. We need this computation:

\[ 1 = \beta = [ab] = a^{\omega \beta}b^{\omega} \quad \text{since } G \text{ is abelian,} \]

So $\omega \beta \equiv \alpha$. Since $\beta \perp \alpha$, necessarily $\omega \equiv \alpha$.

Similarly, $\omega \equiv \beta$. So $\omega \equiv \alpha \beta$, by co-prime-ness.

The general case. Suppose $g_1$ and $g_2$ are elements whose orders, $\gamma_1$ and $\gamma_2$, are not necessarily co-prime.

For each prime $p$, let $e_j = e_j(p)$ be the largest exponent such that $p^{e_j} \equiv \gamma_j$. Define the integers $N_1$ and
$N_2$ as the following products over all primes $p$:

$\gamma := \text{LCM}(\gamma_1, \ldots, \gamma_L)$, so

$$\gamma = \text{Ord}(b) \iff \#G,$$

so every element of $G$ has period $\beta$. Thus $\#G \leq \beta$, since $G$ is order-constrained. Consequently, the cyclic subgroup generated by $b$ is all of $G$.

**Questions/Exercises**

Note that a commutative ring $\Gamma$ without zero-divisors (an integral domain) has this property: A polynomial of degree $n$ can have at most $n$ roots. (First extend $\Gamma$ to its field of fractions, then use synthetic division. Since no zero-divisors, all roots must appear in the factorization obtained.)

7a: **Lemma.** A finite ring $\Gamma$ without [non-trivial] zero-divisors is necessarily a division-ring. (Each non-zero element has a reciprocal.)

**Proof.** Fix a non-zero $b \in \Gamma$. The map $x \mapsto xb$ is injective ($xb = yb$ implies $x - yb = 0$, etc.) Since $\Gamma$ is finite, $x \mapsto xb$ is onto. So $b$ has a left-inverse.

7b: **Question.** This leaves open the question: Are there non-commutative finite division rings? We can’t apply the Cyclic Theorem because we can’t use synthetic division (at least, not directly) to show that the multiplicative group is order-constrained.

What do you think? (See wedderburn-thm.latex for an answer.)

---

**Primitive Roots**

Each posint $N$ yields an abelian (multiplicative) group $\Phi(N)$. If this group is cyclic then each of its generators is called a “primitive root mod $N$” or an $N$-primroot. There are $\varphi(\varphi(N))$ of these primroots.

The foregoing tells us that each prime $p$ has primitive roots, indeed, has $\varphi(p^\alpha) \equiv \varphi(p-1)$ of them. One goal of this section is the result below. For won’t of a better term, a posint $N$ is cyclicish if $N$ has a primroot, that is, if $\{\Phi(N), \cdot, 1\}$ is a cyclic group.

8: **Primroot Theorem.** A posint $N$ is cyclicish IFF: Either $N = 1, 2, 4$ or $N = p^\alpha$ or $N = 2p^\alpha$ for some oddprime $p$ and posint $\alpha$.

**Remark.** The set of cyclicish numbers is sealed under factors, courtesy (2*).

Evidently $-1$ is a primroot mod 1, 2, 4. On the other hand, modulo $8$ each member of

$$\{\pm 1, \pm 3\} \quad \text{note} \quad \Phi(8)$$

is an involution (under multiplication). So $8$ is not cyclicish and thus neither are the higher powers of two.

Suppose we factor $N = J \cdot K$ into co-prime posints. Then the Chinese Remainder Thm gives a ring-isom $\mathbb{Z}_N \cong \mathbb{Z}_J \times \mathbb{Z}_K$ and hence a group-isomorphism $\Phi:

$$\Phi(N) \cong \Phi(J) \times \Phi(K).$$

The only posints with odd Euler $\varphi$-value are 1 and 2. So co-prime $J, K \equiv 3$ must have $\Phi(J)$ and $\Phi(K)$ both even; in which case RhS(I) fails$^\dagger$ to be cyclic. So the only $N (\neq 1, 2, 4)$ which does not permit such a bad factorization is: $J = 1, 2$ and $K$ is a power of an oddprime.

To prove (8), consequently, we need but establish that each $p^\alpha$ has a primroot. [The case of $2 \cdot p^\alpha$ is immediate, courtesy the (1) group-iso $\Phi(2p^\alpha) \rightarrow \Phi(2) \times \Phi(p^\alpha)$, since $\Phi(2)$ is the trivial gp.]

$^\dagger$The product group has at least two elements of order-2, but an even-cardinality cyclic group has a unique order-2 elt.
9: Prime-squared Theorem. Fixing a prime \( p \), the group \( \Phi(p^2) \) is cyclic. Equivalently, the number of \( p^2 \)-primroots is
\[
\varphi(\varphi(p^2)) = \varphi(p-1) \cdot [p-1].
\]
Indeed, this strengthening holds.

For each \( p \)-primroot \( g \):

9': The sum \( g + pt \) is a \( p^2 \)-primroot for exactly \( p-1 \) many values of \( t \in [0..p) \).

\[\Box\]

Pf. Below, the symbol \( \equiv \) means congruence \( \mod p^2 \).

Let
\[
\omega = \omega_t := \text{Ord}_{p^2}(g+pt).
\]

Then \( \varphi(p) \mid \omega \), since \( g+pt \) is a \( p \)-primroot. By EFT (well...Lagrange's thm), \( \omega \mid \varphi(p^2) \). Thus
\[
p-1 \mid \omega \mid [p-1]p.
\]

So \( g + pt \) is a \( p^2 \)-primroot \( \iff \omega \equiv [p-1]p \iff \omega \neq p-1 \). Establishing (9') is equivalent to demonstrating:

9'': For at least \( p-1 \) values of \( t \in [0..p) \) we have that \( \omega_t \neq p-1 \).

(Exer: Why equivalent? Pigeon-hole Principle must have something to do with it, but what are the details?)

So we may freely assume that, say, \( \omega_0 = p-1 \), i.e \( g^{p-1} \equiv 1 \), in order to prove that the other \( \omega_t \neq p-1 \), i.e to prove: For each \( t \in [1..p) \),

9a:
\[
[g+pt]^{p-1} - 1 \neq 0.
\]

By the Binomial Thm, LhS(9a) equals
\[
[g^{p-1} - 1] + g^{p-2} \cdot \binom{p-1}{1} g^1 t^1 + g^{p-3} \cdot \binom{p-1}{2} g^2 t^2 + \ldots + g^0 \cdot \binom{p-1}{p-1} g^{p-1} t^{p-1}.
\]

The first and third lines are divisible by \( p^2 \). (Why?)

Thus
\[
\text{LhS}(9a) \equiv [g^{p-2} \cdot [p-1] t] \cdot p,
\]
and we want to show this not divisible by \( p^2 \).

Dividing the above by \( p \), our objective becomes \( g^{p-2} \cdot [p-1] \cdot t \not\equiv p \). This latter is true since \( g \not\equiv p \) and \( t \not\equiv p \), since \( t \neq 0 \).

\[\Box\]
Primitive roots for powers higher than two.

Fix integers \( g \) and \( D \) and \( N \geq 2 \). Each exponent \( \alpha \in [D, \infty) \) yields a proposition

\[
Q_g(\alpha) : \quad g^{N^{\alpha-D}} \equiv \begin{cases} 1 \pmod{N^\alpha} \\ \neq 1 \pmod{N^{\alpha+1}} \end{cases},
\]

which may be true or false.

10: Lifting Lemma. Fix \( N, D, g, \alpha \) from above.

i: If \( \alpha \geq 2 \) then \( Q_g(\alpha) \implies Q_g(\alpha+1) \).

ii: If \( N \) is oddprime then \( Q_g(1) \implies Q_g(2) \).

\[ \blacksquare \]

Proof. Let \( \beta := \alpha + 1 \) and \( \gamma := \beta + 1 \); so \( \alpha, \beta, \gamma \) are three consecutive integers. Assume \( Q_g(\alpha) \); this implies that

\[
g^{N^{\beta-D}} = 1 + N^\alpha t, \quad \text{for some } t \nmid N.
\]

From this, our goal is to derive \( Q_g(\beta) \). Well

\[
g^{N^{\beta-D}} = [1 + N^\alpha t]^N
\]

\[
= 1 + (N)N^\alpha t + \sum_{j=2}^{N} (N_j)N^j \alpha t^j,
\]

by the Binomial Thm. Rewriting

10a: \( g^{N^{\beta-D}} = 1 + N^\beta t + \left(\frac{N}{2}\right)N^{2\alpha} t^2 + \ldots + \left(\frac{N}{N}\right)N^{N\alpha} t^N \).

Factoring out \( N^{2\alpha} \) gives

10b: \( g^{N^{\beta-D}} = 1 + N^\beta t + N^{2\alpha} \). Integer.

Both (i) and (ii) have \( \alpha \geq 1 \), so \( 2\alpha \geq \beta \). Thus

\[ \text{Rhs}(10b) \equiv 1 \pmod{N^\beta}. \]

That is, the upper line of proposition \( Q_g(\beta) \) holds.

**Non-congruence.** Let \( \equiv \equiv \) mean \([\text{modulo } N^\gamma]\). Since \( t \nmid N \), establishing that \( \text{Rhs}(10a) \not\equiv 1 \) will follow from

\[
*: \quad g^{N^{\beta-D}} \equiv ? 1 + [N^\beta \cdot t].
\]

The \( \alpha \geq 2 \) case is immediate, since \( 2\alpha \geq \gamma \) and so \( \text{Rhs}(10b) \equiv 1 + N^\beta t \).

For the \( \alpha=1 \) case, our goal becomes

****: \( g^{N^{2-D}} \equiv ? 1 + N^2 \cdot t \),

where here, our \( \equiv \equiv \) means modulo \( N^3 \). We can write \( \text{Rhs}(10a) \) as \( 1 + N^2 t + A + B \), where

\[
A := \left(\frac{N}{2}\right)N^{2\alpha} t^2 + \left(\frac{N}{3}\right)N^{3\alpha} t^3 + \ldots + \left(\frac{N}{N-1}\right)N^{N\alpha-1} t^{N-1};
\]

\[
B := \left(\frac{N}{N}\right)N^{N\alpha} t^N.
\]

But \( N^N \equiv 0 \), since exponent \( N \geq 3 \). Thus \( B \equiv 0 \).

Lastly, \( N \) is prime so \( \left(\frac{N}{\ell}\right) \equiv \frac{1}{N} \equiv \frac{1}{N^\ell} \), for each \( \ell \in [2..N] \).

Hence \( \left(\frac{N}{\ell}\right) \cdot N^\ell \equiv 0 \). Thus \( A \equiv 0 \).

\[ \blacksquare \]

10c: Appl. Fixing an oddprime \( p \), let’s use the Lifting lemma to get our hands on primitive roots mod \( p^\alpha \). The map \( x \mapsto (x)_{p^\alpha-1} \) from \( \Phi(p^\alpha) \to \Phi(p^\alpha-1) \) is a surjective group homomorphism. So if \( h \) is a \( p^\alpha \)-primroot then it is a primroot mod all lower powers, \( \alpha, \beta, \gamma \).

We’d like to go in the other direction and lift primroots \( h \). Let’s examine the \( Q_h(\alpha) \) property, above (10), when \( N := p \) and \( D := 1 \) and \( g := h^{p-1} \).

Notice that \( g^{N^{\alpha-D}} \) equals \( h^{p-1} \cdot p^{\alpha-1} \), i.e. \( h^{\varphi(p^\alpha)} \).

For \( \alpha = 1, 2, \ldots \), assertion \( Q_g(\alpha) \) is equivalent to

\[
\widetilde{Q}_h(\alpha) : \quad h^{\varphi(p^\alpha)} \equiv \begin{cases} 1 \pmod{p^\alpha} \\ \neq 1 \pmod{p^{\alpha+1}} \end{cases}.
\]

Of course, if \( h \) is known to be \( \perp p \), then \( \widetilde{Q}_h(\alpha) \) is equivalent to

\[
R_h(\alpha) : \quad h^{\varphi(p^\alpha)} \neq p^{\alpha+1} 1,
\]

since the top line of \( \widetilde{Q}_h(\alpha) \) is EFT.

\[ \blacksquare \]

10d: Corollary (of the Lifting lemma). Suppose \( p \) is prime and \( h \perp p \). Then

\[
R_h(1) \implies R_h(2) \implies R_h(3) \implies R_h(4) \implies \ldots,
\]

where implication (*) holds when \( p \) is odd.

\[ \blacksquare \]
Remark. Trivially $\varphi(p^{\alpha + 1})$ does not divide $\varphi(p^\alpha)$, so
11:  [Integer $h$ is a $p^{\alpha + 1}$-primroot] $\implies R_h(\alpha)$
for each $\alpha \geq 0$.

Remark. The following thm, together with Prime-squared Thm (9), will establish the Primroot Theorem.

12: Primroot Lifting Thm. Consider an oddprime $p$. If integer $h$ is a $p^i$-primroot for some $i \geq 2$, then $h$ is a primroot mod all powers $\{p, p^2, p^3, p^4, \ldots\}$. \hfill $\Box$

Proof. Let $\eta_\alpha := \text{Ord}_{p^\alpha}(h)$, i.e the (multiplicative) group $\Phi(p^\alpha)$. So $\eta_1 \equiv \eta_2 \equiv \eta_3 \equiv \ldots$, since $\Phi(p^{\alpha - 1})$ is a quotient-group of $\Phi(p^\alpha)$. Our goal is to proof that $\eta_\alpha$ equals $\varphi(p^\alpha)$, for each $\alpha \geq 3$, given that
\[
\left\lfloor \eta_2 = \varphi(p^2) \right\rfloor \quad \text{the boxed is the weakest form of the hypothesis.}
\]
Proceeding by induction, suppose $\eta_\alpha = \varphi(p^\alpha)$ and make $\eta_\beta = \varphi(p^{\beta})$ our objective, where $\beta = \alpha + 1$.
Thus $\varphi(p^\alpha) = \eta_\alpha \equiv \eta_\beta \equiv \varphi(p^{\beta})$, i.e.
\[
[p - 1]p^\alpha  \equiv \eta_\beta  \equiv [p - 1]p^\alpha.
\]
Our goal of $\eta_\beta = [p - 1]p^\alpha$ is thus equivalent to $\eta_\beta \neq [p - 1]p^{\alpha - 1}$, i.e, to $\eta_\beta \nmid \varphi(p^\alpha)$, i.e, to $R_h(\alpha)$.

Finally,
\[
R_h(\alpha) \iff R_h(1) \iff h \text{ is a } p^2\text{-primroot},
\]
courtesy (10d) and (11).

### Structure of $\Phi(2^N)$

For $N = 1, 2, \ldots$, let $G_N$ be the (multiplicative) group $\Phi(2^N)$; so $|G_N| = 2^{N-1}$. [Below, angle-brackets $\langle \rangle$ mean “the subgroup generated by”]

13: PoT Lemma. For each $N \in [2..\infty)$: There exists a posodd $D_N$ such that
\[
\langle\rangle:
\]
\[
5^{2^{N-2}} = 1 + 2^N \cdot D_N.
\]
Let $F_N := \langle\rangle G_N$ and $o_N := |F_N| = \text{Ord}_{G_N}(5)$. Then
\[
\langle\rangle:
\]
\[
o_N = 2^{N-2}.
\]

Group $G_N$ is generated by $\{-1, 5\}$. Indeed,
\[
G_N \text{ is isomorphic to } (\mathbb{Z}_2, +) \times (\mathbb{Z}_{2^{N-2}}, +)
\]
via the map generated by $-1 \mapsto (1, 0)$ and $5 \mapsto (0, 1)$.

Proof of $(\langle\rangle)$: High-school algebra gives
\[
\left(\frac{D_{N+1}}{D_N} = D_N + [D_N]^2 \cdot 2^{N-1}\right) \quad \text{by squaring $(\langle\rangle)$}.
\]
This $D_{N+1}$ odd, since $2^{N-1}$ is even, since $N - 1 \geq 1$. $\blacksquare$

Pf of $(\langle\rangle)$. Equality $(\langle\rangle)$ implies $5^{2^{N-1}} \equiv 2^{N+1}$
1. I.e, $o_{N+1} \equiv 2^{N-1}$. So statement $(\langle\rangle)$ is equivalent to showing that $5^{2^{N-2}}$ is not congruent to $1$, modulo $2^{N+1}$.

Now $D_N$ is odd, so $2^N D_N \equiv 2^{N+1} \cdot 2^N$. By $(\langle\rangle)$, then,
\[
5^{2^{N-2}} \equiv 2^{N+1} + 1 + 2^N.
\]
And this RhS is not mod-$2^{N+1}$ congruent to $1$. $\blacksquare$

Pf of $(\langle\rangle)$. The $F_N$-subgroup, says $(\langle\rangle)$, is half of $G_N$.

Since $-1 \in G_N$ is an involution, and $G_N$ is abelian, assertion $(\langle\rangle)$ is equivalent to showing that $-1$ is not in $F_N$. But were there a $k$ with $[1 + 5^k] \equiv 2^N$, then $[1 + 5^k] \equiv 4$, since $N \geq 2$. But $1 + 5^k \equiv_4 2 \not\equiv_4 0$. $\blacksquare$
Carmichael’s lambda

The \textbf{Carmichael function} \( \lambda: \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \) is a variant of Euler-phi: \( \lambda(N) \) is the smallest posint \( K \) so that:

\[ \forall x \perp N : \ x^K \equiv 1 \pmod{N}. \]

Equivalently, \( \lambda(N) \) is “the \textit{exponent} of group \( (\Phi(N), \cdot, 1) \)”.

In the case of a prime, \( \lambda(p) = \varphi(p) = p - 1 \), since \( (\Phi(p), \cdot, 1) \) is cyclic, by Field-Cyclic Thm, (4).

Factoring \( N = p_1^{e_1} \cdots p_L^{e_L} \) into distinct prime-powers gives, by CRT, a group-isomorphism

\[
\lambda(N) = \text{LCM}(\lambda(p_1^{e_1}), \ldots, \lambda(p_L^{e_L})).
\]

When \( N \) is square-free (each \( e_\ell = 1 \) we can specify.

If \( N = p_1 \cdot p_2 \cdots p_L \) with primes distinct, then

\[
\lambda(N) = \text{LCM}(p_1 - 1, p_2 - 1, \ldots, p_L - 1).
\]

\( \lambda() \) is not multiplicative. E.g., \( \lambda(3 \cdot 5) = 2 \neq 4 \cdot 2 = \lambda(3) \cdot \lambda(5) \).

Generalizing Fermat. Posint \( N \) is \textit{fermatish} if

\[
\forall x \perp N : \ x^{N-1} \equiv 1 \pmod{N}.
\]

In other words, \( N \) is fermatish iff

\[
\lambda(N) \mid N-1.
\]

That primes are fermatish was shown by …Fermat.

A fermatish \( N \) is a \textbf{Carmichael number} if it is not prime. Is \( N \) prime? If we test (15) for several values of \( x \), a Carmichael number always fools us.

The first few Carmichael numbers are

\[
\begin{align*}
561 &= 3 \cdot 11 \cdot 17 \\
1105 &= 5 \cdot 13 \cdot 17 \\
1729 &= 7 \cdot 13 \cdot 19.
\end{align*}
\]

16: Korselt’s Thm (1899). A posint \( N \) is fermatish iff \( N \) is square-free and

\[
\psi : \quad p-1 \mid N-1, \quad \text{for each prime } p \mid N.
\]

\textbf{Proof} \( \Leftrightarrow \). By hypothesis, LHS(14') divides \( N-1 \). Hence Rhs(14') \mid N-1. We have (15').

\textbf{Proof} \( \Rightarrow \). We have \( \lambda(N) \mid N-1 \). Since \( N-1 \perp N \), this forces \( \lambda(N) \perp N \). So to show that \( N \) must be square-free, ISTShow \( \frac{p^2 \mid N}{p \mid \lambda(N)} \). So by (14) it suffices to establish

\[
\text{If } e \geq 2 \text{ then } p \nmid \lambda(p^e).
\]

This holds for \( p := 2 \), since the element \(-1\) has order-2 modulo \( 2^e \), once \( e \geq 2 \).

For \( p \) odd, this holds since \( \lambda(p^e) = \varphi(p^e) \), by the Primroot theorem, (8).

We now have (14') —which implies, given a prime \( p \mid N \), that \( p-1 \nmid \lambda(N) \). And \( \lambda(N) \mid N-1 \), since \( N \) is fermatish.

17: Corollary. A posint \( N \) is a Carmichael number iff \( N \) is square-free with (16\( \psi \)), and has at least three prime factors.

\textbf{Pf.} To rule out the two-factor case, FTSOC suppose \( N = pq \) with \( p \neq q \) primes. By hyp, \( p-1 \) divides

\[
N-1 \not\equiv p-1|q + |q-1|.
\]

Hence \( p-1 \nmid q-1 \). By symmetry, \( p-1 \mid q-1 \). Both are posints, so \( p-1 = q-1 \).

\textbf{Slightly generalizing} (14). The Primroot thm implies that \( \lambda(p^e) = \varphi(p^e) \), when \( p \) is an odd prime. Write

\[
N = \tau \cdot p_2^{e_2} \cdots p_L^{e_L},
\]

where \( \tau \) is a PoT, and \( p_2, \ldots, p_L \) are distinct odd-primes. The PoT Lemma says \( \lambda(\tau) \) equals \( \tau/4 \), for \( \tau=8,16,32,\ldots \).

So

\[
\lambda(N) = \text{LCM}(\lambda(\tau), \varphi(p_2^{e_2}), \ldots, \varphi(p_L^{e_L})),
\]

where \( \lambda(1)=\lambda(2)=1 \) and \( \lambda(4)=2 \).

When \( N \) has at least one odd prime then

\[
\lambda(N) = \text{LCM}(2, \lambda(\tau), H_1, \ldots, H_L, [p_2^{b_2} \cdots p_L^{b_L}]),
\]

where \( b_\ell := e_\ell - 1 \), and \( H_\ell := [p_\ell - 1]/2 \).
§Index, with symbols and abbrevs at the End

Carmichael function, 7
Carmichael number, 7
Cyclicish, 3
division-ring, 3
Euler phi, 1
Fermatisch, 7
Integral domain, 3
NZM, 4
Order, 1
Order-constrained, 2
Period
of an element, 1
PoT, 1
Primitive root, 3