

**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/>
17 November, 2017 (at 12:06)

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 $k \blacktriangleright n$ for “ k divides n ”. Its negation $k \not\blacktriangleright n$ means “ k does not divide n .” Use $n \blacktriangleright k$ and $n \not\blacktriangleright k$ for “ n is/is-not a multiple of k .” Finally, for p a prime and E a natnum: Use double-verticals, $p^E \blacktriangleright n$, to mean that E is the **highest** power of p which divides n . Or write $n \blacktriangleright p^E$ 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 Φ_N for the set $\{r \in [1..N] \mid r \perp N\}$. The cardinality $\varphi(N) := |\Phi_N|$ is the **Euler phi function**. (So $\varphi(N)$ is the cardinality of the multiplicative group, Φ_N , in the \mathbb{Z}_N ring.) Use **EFT** for the Euler-Fermat Thm, which says: *Suppose that integers $b \perp N$, with N positive. Then $b^{\varphi(N)} \equiv_N 1$.*

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 $(S, \cdot, 1)$ is a semigroup [written multiplicatively, with unit] which is not necessarily abelian, nor finite. Fix a $z \in S$. A posint \mathbf{n} is “**a period** of z ” if $z^{\mathbf{n}} = 1$. Let

$$\text{Per}_S(z) := \{\mathbf{n} \in \mathbb{Z}_+ \mid z^{\mathbf{n}} = 1\}.$$

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

Of course, when z has finite order, \mathbf{n} , then z is invertible, since $z \cdot z^{\mathbf{n}-1}$ equals 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 z has a mod- N multiplicative-order IFF $z \perp N$. Let $\text{Ord}_N(z)$ denote this order, and $\text{Per}_N(z)$ the set of periods.

1: Prop’n. *Suppose posints $K \blacktriangleright N$ and $z \perp N$. Then $\text{Ord}_K(z) \blacktriangleright \text{Ord}_N(z)$.* ♦

Proof. Let $k := \text{Ord}_K(z)$. BÄ©zout’s thm implies that $\text{Per}_K(z)$ equals $k\mathbb{Z}$. For an $n \in \text{Per}_N(z)$, note, $[z^n - 1] \blacktriangleright N \blacktriangleright K$. So $n \in k\mathbb{Z}$. ♦

Given a ring-hom $h: \Gamma \rightarrow \Gamma'$, easily the forward 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, $h: \mathbb{Z} \rightarrow \mathbb{Z}_5$ by $x \mapsto \langle x \rangle_5$.

2: Prop’n. *Fix posints $N \blacktriangleright K$. Let $h: \mathbb{Z}_N \rightarrow \mathbb{Z}_K$ 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*

*****: $\Phi(N) \text{ cyclic} \implies \Phi(K) \text{ cyclic}.$

Hence, if \mathbf{g} is an N -primroot, then $\langle \mathbf{g} \rangle_K$ 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 $f: \mathbb{Z}_N \rightarrow \mathbb{Z}_K \times \mathbb{Z}_Q$ by $x \mapsto (\langle x \rangle_K, \langle x \rangle_Q)$. *Exercise:* The set of units in $\mathbb{Z}_K \times \mathbb{Z}_Q$ is $\Phi(K) \times \Phi(Q)$. Hence, for $z \in \Phi(K)$: The set $h^{-1}(z)$ 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 \widetilde{K} be the product, over those primes $p \blacktriangleright K$, of p^{ℓ_p} , where $p^{\ell_p} \blacktriangleright N$. Evidently $\widetilde{K} \perp N/\widetilde{K}$.

A K -unit z evidently has $z \perp \widetilde{K}$. By the above special case, z has a “ \widetilde{K} -lift” $z + t\widetilde{K}$ which is co-prime to N . And it is also a K -lift, since $K \blacktriangleright \widetilde{K}$. ♦

Fields

Let \mathbf{F} be a field, and let G be its multiplicative subgroup; that is, $G := \mathbf{F} \setminus \{0\}$. Fix n and consider all elements in \mathbf{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 \mathbf{F} , a finite field with $G := \mathbf{F} \setminus \{0\}$ its multiplicative subgroup. Let $L := |G|$. Then G is cyclic, that is, $(G, \cdot, 1)$ is group-isomorphic to $(\mathbb{Z}_L, +, 0)$. \diamond

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. \diamond

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

$$5a: \quad \sum_{\substack{m \bullet L \\ m \in [1..L]}} \psi_G(m) = |G| = L.$$

Now consider an m for which $\psi(m)$ is not zero; so there is an element $\mathbf{b} \in G$ whose order is m . This \mathbf{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

$$5b: \quad \text{For each } m: \quad \psi_G(m) \leq \varphi(m).$$

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

$$5a': \quad \sum_{\substack{m \bullet L \\ m \in [1..L]}} \varphi(m) = |\mathbb{Z}_L| = L.$$

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 . \diamond

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 $\mathbf{a}, \mathbf{b} \in S$, the Lcm of their orders, α and β , is itself the order of some element in sub-semigroup $\langle \mathbf{a}, \mathbf{b} \rangle \subset S$.

In the $\alpha \perp \beta$ special-case, then element \mathbf{ab} has order $\alpha\beta$. \diamond

Proof. WLOG both elements have finite order.

When $\alpha \perp \beta$. Write $\omega := \text{Ord}(\mathbf{ab})$. Since $[\mathbf{ab}]^{\alpha\beta}$ equals $[\mathbf{a}^\alpha]^\beta \cdot [\mathbf{b}^\beta]^\alpha = 1 \cdot 1 = 1$, we have that $\omega \bullet \alpha\beta$. Thus ISTShow that $\boxed{\omega \bullet \alpha\beta}$.

We need this computation:

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

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

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

The general case. Suppose \mathbf{g}_1 and \mathbf{g}_2 are elements whose orders, γ_1 and γ_2 , are not necessarily co-prime.

For each prime \mathbf{p} , let $e_j = e_j(\mathbf{p})$ be the *largest* exponent such that $\mathbf{p}^{e_j} \bullet \gamma_j$. Define the integers N_1 and

N_2 as the following products over all primes p :

N_1 is the product of all $p^{e_1(p)}$ such that $e_1(p) \geq e_2(p)$;

and

N_2 is the product of all $p^{e_2(p)}$ such that $e_1(p) < e_2(p)$.

Automatically, each N_j divides γ_j and so the element $[\mathbf{g}_j]^{\gamma_j/N_j}$ has order N_j . By their definition, $N_1 \perp N_2$. Therefore the foregoing special case tells us that there is an element of order $N_1 \cdot N_2$. And the product $N_1 N_2$ equals $\text{Lcm}(\gamma_1, \gamma_2)$. ♦

Proof: Abelian version of the Cyclic Theorem, (5). Let $\mathbf{g}_1, \dots, \mathbf{g}_L$ be an enumeration of all the elements of G and let $\gamma_1, \dots, \gamma_L$ denote their orders. By using the LCM Lemma $L-1$ times we conclude that there is an element $\mathbf{b} \in G$ whose order is

$$\beta := \text{Lcm}(\gamma_1, \dots, \gamma_L), \text{ so}$$

$$\beta = \text{Ord}(\mathbf{b}) \mid \#G.$$

So every element of G has period β . Thus $\#G \leq \beta$, since G is order-constrained. Consequently, the cyclic subgroup generated by \mathbf{b} is all of G . ♦

Questions/Exercises

Note that a commutative ring Γ without zero-divisors (an *integral domain*) has this property: *A polynomial of degree n can have at most n roots.* (First extend Γ 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 Γ without [non-trivial] zero-divisors is necessarily a **division-ring**. (Each non-zero element has an inverse.)* ♦

Proof. Fix a non-zero $b \in \Gamma$. The map $x \mapsto xb$ is injective ($xb = yb$ implies $[x - y]b = 0$, etc.) Since Γ 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.tex` 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 $\varphi(\varphi(p)) = \varphi(p-1)$ of them. One goal of this section is the result below. For want 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 α .* ♦

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

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

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-iso $\mathbb{Z}_N \cong \mathbb{Z}_J \times \mathbb{Z}_K$ and hence a group-isomorphism

$$\dagger: \quad \Phi(N) \cong \Phi(J) \times \Phi(K).$$

The only posints with odd Euler φ -value are 1 and 2 . So co-prime $J, K \geq 3$ must have $\Phi(J)$ and $\Phi(K)$ both even; in which case $\text{Rhs}(\dagger)$ *fails*^{♥1} 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^α has a primroot.* [The case of $2 \cdot p^\alpha$ is immediate, courtesy the (\dagger) group-iso $\Phi(2p^\alpha) \rightarrow \Phi(2) \times \Phi(p^\alpha)$, since $\Phi(2)$ is the trivial gp.] □

^{♥1}The product group has at least two elements of order-2, but a 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

$$\varphi(\varphi(p^2)) \stackrel{\text{note}}{=} \varphi(p-1) \cdot [p-1].$$

Indeed, this strengthening holds.

For each p -primroot g :

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

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 $\omega = [p-1]p$ IFF $\omega \neq p-1$. Establishing ('?') is equivalent to demonstrating:

g'' : 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 $t \in [1..p)$,

$$9a: \quad [g+pt]^{p-1} - 1 \not\equiv 0.$$

By the Binomial Thm, LhS(9a) equals

$$\begin{aligned} & [g^{p-1} - 1] + \\ & g^{p-2} \cdot \binom{p-1}{1} p^1 t^1 + \\ & g^{p-3} \cdot \binom{p-1}{2} p^2 t^2 + \dots + g^0 \cdot \binom{p-1}{p-1} p^{p-1} t^{p-1}. \end{aligned}$$

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

$$\text{LhS}(9a) \equiv [g^{p-2} \cdot [p-1] \cdot t] \cdot p,$$

and we want to show this not divisible by p^2 .

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

Remark. [N.B: The preceding proof works for all primes, including $p = 2$.] The *Niven, Zuckerman, Montgomery* text ("NZM") has a neat proof of (9), by means of Hensel's lemma. \square

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

$$Q_g(\alpha): \quad g^{N^{\alpha-D}} \text{ is } \left\{ \begin{array}{l} \equiv 1 \text{ modulo } N^\alpha \\ \text{and is} \\ \not\equiv 1 \text{ modulo } N^{\alpha+1} \end{array} \right\},$$

which may be true or false.

10: Lifting Lemma. Fix N, D, g, α from above.

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

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

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

$$g^{N^{\alpha-D}} = 1 + N^\alpha t, \quad \text{for some } t \not\vdash N.$$

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

$$\begin{aligned} g^{N^{\beta-D}} &= [1 + N^\alpha t]^N \\ &= 1 + \binom{N}{1} N^\alpha t + \sum_{j=2}^N \binom{N}{j} N^{j\alpha} t^j, \end{aligned}$$

by the Binomial Thm. Rewriting

$$10a: \quad g^{N^{\beta-D}} = 1 + N^\beta t + \binom{N}{2} N^{2\alpha} t^2 + \dots + \binom{N}{N} N^{N\alpha} t^N.$$

Factoring out $N^{2\alpha}$ gives

$$10b: \quad g^{N^{\beta-D}} = 1 + N^\beta t + N^{2\alpha} \cdot \text{Integer}.$$

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 $\boxed{\text{modulo } N^\gamma}$. Since $t \not\vdash N$, establishing that $\text{RHS}(10a) \not\equiv 1$ will follow from

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

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

$$**: \quad g^{N^{2-D}} \stackrel{?}{\equiv} 1 + N^2 \cdot t,$$

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

$$\begin{aligned} A &:= \binom{N}{2} N^2 t^2 + \binom{N}{3} N^3 t^3 + \dots + \binom{N}{N-1} N^{N-1} t^{N-1}; \\ B &:= \binom{N}{N} N^N t^N. \end{aligned}$$

But $N^N \equiv 0$, since exponent $N \geq 3$. Thus $B \equiv 0$. Lastly, N is prime so $\binom{N}{\ell} \not\vdash N$, for each $\ell \in [2 .. N)$. Hence $\binom{N}{\ell} \cdot N^\ell \equiv 0$. Thus $A \equiv 0$. \blacklozenge

10c: Appl. Fixing an oddprime p , let's use the Lifting lemma to get our hands on primitive roots mod p^α . The map $x \mapsto \langle x \rangle_{p^{\alpha-1}}$ from $\Phi(p^\alpha)$ to $\Phi(p^{\alpha-1})$ is a surjective group homomorphism. So if h is a p^α -primroot then it is a primroot mod all lower powers, $p^{\alpha-1}, p^{\alpha-2}, \dots, p^2, p^1$.

We'd like to go in the other direction and lift primroots h . Let's examine the $Q_g(\alpha)$ property, above (10), when $N := p$ and $D := 1$ and $g := h^{p-1}$. Notice that $g^{N^{\alpha-D}}$ equals $h^{[p-1]p^{\alpha-1}}$, i.e. $h^{\varphi(p^\alpha)}$.

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

$$\tilde{Q}_h(\alpha): \quad h^{\varphi(p^\alpha)} \text{ is } \left\{ \begin{array}{l} \equiv 1 \text{ modulo } p^\alpha \\ \text{and is} \\ \not\equiv 1 \text{ modulo } p^{\alpha+1} \end{array} \right\}.$$

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

$$R_h(\alpha): \quad h^{\varphi(p^\alpha)} \not\equiv_{p^{\alpha+1}} 1,$$

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

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

$$R_h(1) \stackrel{*}{\implies} R_h(2) \implies R_h(3) \implies R_h(4) \implies \dots,$$

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

Remark. Trivially $\varphi(p^{\alpha+1})$ does not divide $\varphi(p^\alpha)$, so

$$11: \quad [\text{Integer } \mathbf{h} \text{ is a } p^{\alpha+1}\text{-primroot}] \implies R_{\mathbf{h}}(\alpha)$$

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 \mathbf{h} is a p^i -primroot for some $i \geq 2$, then \mathbf{h} is a primroot mod all powers p, p^2, p^3, p^4, \dots ◇

Proof. Let $\eta_\alpha := \text{Ord}_{p^\alpha}(\mathbf{h})$, i.e in the (multiplicative) group $\Phi(p^\alpha)$. So $\eta_1 \bullet \eta_2 \bullet \eta_3 \bullet \dots$, since $\Phi(p^{\alpha-1})$ is a quotient-group of $\Phi(p^\alpha)$. Our goal is to prove that η_α equals $\varphi(p^\alpha)$, for each $\alpha \geq 3$, given that $\boxed{\eta_2 = \varphi(p^2)}$; the boxed is the weakest form of the hypothesis.

Proceeding by induction, suppose $\eta_\alpha = \varphi(p^\alpha)$ and make $\eta_\beta \stackrel{?}{=} \varphi(p^\beta)$ our objective, where $\beta := \alpha + 1$. Thus $\varphi(p^\alpha) = \eta_\alpha \bullet \eta_\beta \bullet \varphi(p^\beta)$, ie.

$$[p-1]p^{\alpha-1} \bullet \eta_\beta \bullet [p-1]p^\alpha.$$

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 $R_{\mathbf{h}}(\alpha)$.

Finally,

$$R_{\mathbf{h}}(\alpha) \Leftarrow R_{\mathbf{h}}(1) \Leftarrow [\mathbf{h} \text{ is a } p^2\text{-primroot}],$$

courtesy (10d) and (11). ◇

Structure of $\Phi(2^N)$

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

13: PoT Lemma. For each $N \in [2.. \infty)$: There exists a posodd D_N such that

$$\dagger_N: \quad 5^{2^{N-2}} = 1 + 2^N \cdot D_N.$$

Let $F_N := \langle 5 \rangle_{G_N}$ and $\mathbf{o}_N := |F_N| = \text{Ord}_{G_N}(5)$. Then

$$\dagger_N: \quad \mathbf{o}_N = 2^{N-2}.$$

Group G_N is generated by $\{-1, 5\}$. Indeed,

G_N is isomorphic to $(\mathbb{Z}_2, +) \times (\mathbb{Z}_{2^{N-2}}, +)$
 13': via the map generated by $-1 \mapsto (1, 0)$ and $5 \mapsto (0, 1)$. ◇

Proof of (\dagger_{N+1}) . High-school algebra gives

$$\boxed{D_{N+1} = D_N + [D_N]^2 \cdot 2^{N-1}}, \text{ by squaring } (\dagger_N).$$

This D_{N+1} odd, since 2^{N-1} is even, since $N-1 \geq 1$. ◇

Pf of (\dagger_{N+1}) . Equality (\dagger_{N+1}) implies $5^{2^{N-1}} \equiv_{2^{N+1}}$

1. I.e, $\mathbf{o}_{N+1} \bullet 2^{N-1}$. So statement $\boxed{\mathbf{o}_{N+1} = 2^{N-1}}$

is equivalent to showing that $5^{2^{N-2}}$ is **not** congruent to 1, modulo 2^{N+1} .

Now D_N is odd, so $2^N D_N \equiv_{2^{N+1}} 2^N$. By (\dagger_N) , then,

$$5^{2^{N-2}} \equiv_{2^{N+1}} 1 + 2^N.$$

And this RhS is *not* mod- 2^{N+1} congruent to 1. ◇

Pf of $(??')$. The F_N -subgroup, says (\dagger_N) , is half of G_N .

Since $-1 \in G_N$ is an involution, and G_N is abelian, assertion $(??')$ is equivalent to showing that -1 is *not* in F_N . But were there a k with $[1 + 5^k] \bullet 2^N$, then $[1 + 5^k] \bullet 4$, since $N \geq 2$. But $1 + 5^k \equiv_4 2 \not\equiv_4 0$. ◇

Carmichael's lambda

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

$$\forall x \perp N: \quad x^K \equiv_N 1.$$

Equivalently, $\lambda(N)$ is the “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 $N = p_1^{e_1} \cdot \dots \cdot p_L^{e_L}$ into *distinct* prime-powers gives, by CRTm, a group-isomorphism

$$14: \quad \begin{aligned} \Phi(N) &\cong \Phi(p_1^{e_1}) \times \dots \times \Phi(p_L^{e_L}). \quad \text{Thus} \\ \lambda(N) &= \text{Lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_L^{e_L})). \end{aligned}$$

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

If $N = p_1 \cdot p_2 \cdot \dots \cdot p_L$ with primes distinct, then

$$14': \quad \lambda(N) = \text{Lcm}(p_1 - 1, p_2 - 1, \dots, p_L - 1).$$

$\lambda()$ is not multiplicative. E.g, $\lambda(3 \cdot 5)$ equals $\text{Lcm}(\lambda(3), \lambda(5)) = \text{Lcm}(2, 4) = 4 \neq 2 \cdot 4$.

Generalizing Fermat. Posint N is *fermatish* if

$$15: \quad \forall x \perp N : \quad x^{N-1} \equiv_N 1.$$

In other words, N is *fermatish* IFF

$$15': \quad \lambda(N) \mid N-1.$$

That primes are *fermatish* was shown by ... Fermat. A *fermatish* N is a **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

$$\begin{aligned} 561 &= 3 \cdot 11 \cdot 17 \quad \text{and} \\ 1105 &= 5 \cdot 13 \cdot 17 \quad \text{and} \\ 1729 &= 7 \cdot 13 \cdot 19. \end{aligned}$$

16: Korselt's Thm (1899). *A posint N is *fermatish* IFF N is square-free and*

$$\forall p : \quad p-1 \mid N-1, \quad \text{for each prime } p \mid N. \quad \diamond$$

Proof (\Leftarrow). By hypothesis, RhS(???) divides $N-1$. Hence LhS(???) $\mid N-1$. We have (???) \diamond

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 If $p^2 \mid N$ then $p \mid \lambda(N)$. By (14) it suffices to establish

$$\text{If } e \geq 2 \text{ then } p \mid \lambda(p^e).$$

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 (???) —which implies, given a prime $p \mid N$, that $p-1 \mid \lambda(N)$. And $\lambda(N) \mid N-1$, since N is *fermatish*. \blacklozenge

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

Pf. To rule out the *two-factor* case, FTSOC suppose $N = pq$ with $p \neq q$ primes. By hyp, $p-1$ divides

$$N-1 \stackrel{\text{note}}{=} [p-1]q + [q-1].$$

Hence $p-1 \mid q-1$. By symmetry, $p-1 \mid q-1$. Both are posints, so $p-1 = q-1$. \blacklozenge

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

$$N = \tau \cdot p_2^{e_2} \cdot \dots \cdot p_L^{e_L},$$

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

$$\lambda(N) = \text{Lcm}(\lambda(\tau), \varphi(p_2^{e_2}), \dots, \varphi(p_L^{e_L})),$$

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

When N has at least one odd prime then

$$\lambda(N) = \text{Lcm}\left(2, \lambda(\tau), H_1, \dots, H_L, [p_2^{b_2} \cdot \dots \cdot p_L^{b_L}]\right),$$

where $b_\ell := e_\ell - 1$, and $H_\ell := [p_\ell - 1]/2$. \square

§Index, with symbols and abbrevs at the End

Carmichael function, **6**

Carmichael number, **6**

division ring, **3**

fermatish, **6**

GCoDiLiCo, **1**

integral domain, **3**

NZM, **4**

order, **1**

order-constrained, **1**

period

 of an element, **1**

PoT, **1**

primitive root, **3**

primrootish, **3**

Filename: Problems/Algebra/finite-fields.tex
As of: Friday 10Mar2006. Typeset: 17Nov2017 at 12:06.