

Partial Theorem List (preliminary)

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 27 July, 2018 (at 22:27)

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.] Easily, $\varphi(p^L) = [p-1] \cdot p^{L-1}$, for prime p and posint L .

Use **EFT** for the Euler-Fermat Thm, which says: Suppose that integers $b \perp N$, with N positive. Then $b^{\varphi(N)} \equiv_N 1$.

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

1: Euclidean Algorithm Thm (EuclAlg). Given B and C , not both zero, let $G := \text{Gcd}(B, C)$. Then there are integers s and t , called **Bézout multipliers**, with

$$1a: \quad Bs + Ct = G.$$

More generally, given integers B_1, \dots, B_L not all zero, there exists a **Bézout tuple** $(s_\ell)_{\ell=1}^K$ such that

$$1b: \quad \sum_{\ell=1}^K B_\ell \cdot s_\ell = \text{Gcd}(B_1, \dots, B_K).$$

Returning to the $L = 2$ case, pick one pair (s_0, t_0) fulfilling (1a). Then the set of all such pairs is precisely $\{(s_k, t_k)\}_{k \in \mathbb{Z}}$, where

$$1c: \quad \begin{aligned} s_k &:= s_0 + k \cdot \frac{C}{G}, \\ t_k &:= t_0 - k \cdot \frac{B}{G}. \end{aligned} \quad \diamond$$

Primes vs. Irreducibles. Consider a commutative ring $(\Gamma, +, 0, \cdot, 1)$. An elt $\alpha \in \Gamma$ is a **zero-divisor** (abbrev **ZD**) if there exists a *non-zero* $\beta \in \Gamma$ st. $\alpha\beta = 0$. In contrast, an element $u \in \Gamma$ is a **unit** if $\exists w \in \Gamma$ st. $u \cdot w = 1$. (This w is the “multiplicative inverse” of u , is unique, and is often written u^{-1} .) **Exer 1:** In an arbitrary ring Γ , the set $\text{ZD}(\Gamma)$ is *disjoint* from $\text{Units}(\Gamma)$.

An element α is:

- i:* Γ -**irreducible** if α is a non-unit, non-ZD, such that for each Γ -factorization $\alpha = x \cdot y$, either x or y is a Γ -unit. [Restating, using the definition below: Either $x \approx 1, y \approx \alpha$, or $x \approx \alpha, y \approx 1$.]
- ii:* Γ -**prime** if α is a non-unit, non-ZD, such that for each pair $c, d \in \Gamma$: If $\alpha \spadesuit [c \cdot d]$ then *either* $\alpha \spadesuit c$ or $\alpha \spadesuit d$.

Associates. Ring-elts α and β are **associates**, written $\alpha \sim \beta$, if $\alpha \spadesuit \beta$ and $\alpha \spadesuit\!\!\spadesuit \beta$ [i.e., $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$]. They are **strong associates**, written $\alpha \approx \beta$, if there exists a unit u st. $\beta = u\alpha$.

Ex 2: Prove *Strong-Assoc* \Rightarrow *Assoc*.

Ex 3: If $\alpha \sim \beta$ and $\alpha \notin \text{ZD}$, then α, β are **strong associates**.

Ex 4: In \mathbb{Z}_{10} , zero-divisors 2, 4 are associates. Are they strong associates?

Ex 5: With $d \spadesuit \alpha$, prove: *If α is a non-ZD, then d is a non-ZD.* And: *If α is a unit, then d is a unit.*

2: Lemma. In a commRing Γ , each prime α is irreducible. \diamond

Proof. Consider factorization $\alpha = xy$. Since $\alpha \spadesuit xy$, WLOG $\alpha \spadesuit x$, i.e. $\exists c$ with $\alpha c = x$. Hence

$$*: \quad \alpha = xy = \alpha cy.$$

By defn, $\alpha \notin \text{ZD}$. We may thus cancel in (*), yielding $1 = cy$. So y is a unit. \diamond

There are rings^{♥1} with irreducible elements p which are nonetheless not prime. However...

^{♥1}Consider the ring, Γ , of polys with coefficients in \mathbb{Z}_{12} . There, $x^2 - 1$ factors as $[x - 5][x + 5]$ and as $[x - 1][x + 1]$. Thus none of the four linear terms is prime. Yet each is Γ -irreducible. (Why?) This ring Γ has zero-divisors (suck!), but there are natural subrings of \mathbb{C} where $\text{Irred} \neq \text{Prime}$.

3: Lemma. Suppose commRing Γ satisfies the Bézout condition, that each Gcd is a linear-combination. Then each irreducible α is prime. \diamond

Proof. Suppose $\alpha \mid xy$ and WLOG $\alpha \nmid x$. Let $g := \text{Gcd}(\alpha, x)$. Were $g \approx \alpha$, then $\alpha \mid g \mid x$, a contradiction. Thus, since α is irreducible, our $g \approx 1$.

Bézout produces $S, T \in \Gamma$ with

$$1 = S\alpha + Tx. \text{ Hence}$$

$$*: \quad y = S\alpha y + Txy = Sy\alpha + Txy.$$

By hyp, $\alpha \mid xy$, hence α divides RhS(*). So $\alpha \mid y$. \diamond

Example where $\sim \neq \approx$. Here a modification of an example due to Kaplansky.

Let Ω be the ring of real-valued cts fncs on $[-2, 2]$. Define $\mathcal{E}, \mathcal{D} \in \Omega$ by: For $t \geq 0$:

$$\mathcal{E}(t) = \mathcal{D}(t) := \begin{cases} t-1 & \text{if } t \in [1, 2] \\ 0 & \text{if } t \in [0, 1] \end{cases}.$$

And for $t \leq 0$ define

$$\mathcal{E}(t) := \mathcal{E}(-t) \quad \text{and} \quad \mathcal{D}(t) := -\mathcal{D}(-t).$$

[So \mathcal{E} is an Even fnc; \mathcal{D} is odd.] Note $\mathcal{E} = f\mathcal{D}$ and $\mathcal{D} = f\mathcal{E}$, where

$$f(t) := \begin{cases} 1 & \text{if } t \in [1, 2] \\ t & \text{if } t \in [-1, 1] \\ -1 & \text{if } t \in [-2, -1] \end{cases}.$$

Hence $\mathcal{E} \sim \mathcal{D}$. [This f is not a unit, since $f(0) = 0$ has no reciprocal. However, f is a non-ZD: For if $fg = \mathbf{0}$, then g must be zero on $[-2, 2] \setminus \{0\}$. Cty of g then forces $g = \mathbf{0}$.]

Could there be a unit $u \in \Omega$ with $u\mathcal{D} = \mathcal{E}$? Well

$$u(2) = \frac{\mathcal{E}(2)}{\mathcal{D}(2)} \stackrel{\text{note}}{=} 1, \quad \text{and} \quad u(-2) = \frac{\mathcal{E}(-2)}{\mathcal{D}(-2)} \stackrel{\text{note}}{=} -1.$$

Cty of $u()$ forces u to be zero somewhere on $(-2, 2)$, hence u is not a unit. \square

Convention. Because there are so few units in \mathbb{Z} , it is conventional to just call the appropriate positive numbers “irreducible” or “prime”. To an algebraist, -5 is prime; but it is an associate of 5 , so one can always express arguments in terms of 5 .

4: Lemma. In \mathbb{Z} , each irreducible element p is necessarily prime. \diamond

Pf. With $p \mid c \cdot d$, suppose that p does not divide d . Thus $g := \text{Gcd}(p, d)$ cannot be p . So g is a proper divisor of our irreducible p , so g must be 1 .

By EuclAlg there are Bézout multipliers S, T such that $1 = pS + dT$. Multiplying by c , then, yields

$$c = cpS + cdT.$$

But each term on RhS is divisible by p . So $c \mid p$. \diamond

5a: Fermat’s Little Thm (FLiT). For p prime and each $\mathbf{b} \in \mathbb{Z}$:

$$\mathbf{b}^p \equiv_p \mathbf{b}. \quad \diamond$$

5b: Euler-Fermat Thm (EFT). For $N \in \mathbb{Z}_+$ and $\mathbf{b} \perp N$,

$$\mathbf{b}^{\varphi(N)} \equiv_N 1. \quad \diamond$$

Proof. Define $f: \Phi_N \rightarrow \Phi_N$ by $f(x) := \langle x\mathbf{b} \rangle_N$. Since $\mathbf{b} \perp N$, our f is injective, hence (by PHP) f is a bijection. So we can write $V := \prod(\Phi_N)$ as

$$*: \quad \prod_{x \in \Phi_N} f(x) \stackrel{\text{note}}{=} \mathbf{b}^{\varphi(N)} \cdot \prod_{x \in \Phi_N} x = \mathbf{b}^{\varphi(N)} \cdot V,$$

where equality means in the ring \mathbb{Z}_N . Since V is a product of elts coprime to N , our $V \perp N$. So we can cancel out the V in (*) and obtain that $1 \equiv_N \mathbf{b}^{\varphi(N)}$. \diamond

ASIDE. Alternatively, EFT follows from Lagrange’s thm that the order of a subgroup divides the order of the enclosing group. \square

6: Wilson’s Thm. Fix a prime p . Then $\prod(\Phi_p) = -1$ in \mathbb{Z}_p . Alternatively $[p-1]! \equiv_p -1$. \diamond

General abbrevs. OTOH, On the other hand.

WLOG, Without loss of generality.

FTSOC, For The Sake Of Contradiction.

TFAE. The following are equivalent.

ISTShow. It suffices to show.

sqrt, sqroot, square-root.

RHS, RightHand Side (of an equation or inequality).

LHS, LeftHand Side.

More abbrevs. SOTS: Sum-Of-Two-Squares. So $13 = 2^2 + 3^2$ is SOTS. And $25 = 0^2 + 5^2 = 3^2 + 4^2$ is SOTS in two ways.

A integer N is **coprime-SOTS** if *there exist* integers $x \perp y$ st. $x^2 + y^2 = N$. Eg, 20 is SOTS, but is *not* coprime-SOTS. What about 125? Certainly $125 = 10^2 + 25 = 10^2 + 5^2$; but $10 \not\perp 5$, so we still don't know. Noting that $125 = 121 + 4 = 11^2 + 2^2$, and $11 \perp 2$, we conclude that 125 *is* coprime-SOTS.

3POS: An integer n is 3POS if $n \equiv_3 +1$, and is 3NEG if $n \equiv_3 -1$. Similarly, " $n \in 4NEG$ " means $n \equiv_4 -1$.

An odd integer n is 8NEAR if n is mod-8 congruent either to +1 or to -1. Saying " $n \in 8FAR$ " means that $n \equiv_8 \pm 3$. (So -11, 3, 5, 13, 21 are some 8FAR numbers. And -7, 9, 15, 23 \in 8NEAR.)

Theorem abbrevs

QF, Quadratic Formula. UFT, Unique Factorization Thm (also called FTArithm). FLiT, Fermat's Little Thm. FLaT, Fermat's Last Thm (also FLT).

EFT, Euler-Fermat Thm. LST, Legendre-symbol Thm. SOTS Thm; Fermat's Thm characterising which posints are SOTS. PNT, Prime Number Thm. EuclAlg, Euclidean Algorithm.

Standing notation

Use MF to mean "(a) multiplicative function" or "multiplicative".

QR, Quadratic residue. NQR, Non-quadratic residue. For posint m , use m -QR for a mod- m QR, and use m -NQR for a mod- m NQR. E.g "Number -2 is an 11-QR (since $3^2 \equiv_{11} -2$), and +2 is an 11-NQR [since none of $1^2, 2^2, 3^2, 4^2, 5^2$ is $\equiv_2 \pmod{11}$]." Another example: Number 13 is a 51-QR, since $8^2 \equiv_{51} 13$, and $-1 \in \text{NQR}_{51}$. But 6 is neither a QR_{51} *nor* a NQR_{51} , since 6 *fails* to be coprime to 51.

Arith-prog means "arithmetic progression".

Given an odd prime p , let $H = H(p) := \frac{p-1}{2}$. Let $S = S(p)$ be the unique integer st. $S^2 < p < [S + 1]^2$; so $S = \lfloor \sqrt{p} \rfloor$. When p is a 4POS-prime, let $R(p)$ be the unique value $R \in [1 .. H]$ so that $R^2 \equiv_p -1$.

Defn. For a prime p and integer z , the **Legendre-symbol** is written as

$$\left(\frac{z}{p}\right) \text{ or, in email, also as } (z // p).$$

By defn, $\left(\frac{z}{p}\right)$ is +1, if $z \in \text{QR}_p$; is -1, if $z \in \text{NQR}_p$; and is 0, if $z \not\perp p$, i.e $z \mid p$.

An odd integer k is "4POS" if $k \equiv_4 +1$; is 4NEG if $k \equiv_4 -1$; is 8NEAR if $k \equiv_8 \pm 1$ (either); is 8FAR if $k \equiv_8 \pm 3$. □

7: Legendre-symbol Thm. Fix an odd prime p and $H := \frac{p-1}{2}$. Use $\langle \cdot \rangle_p$ for symmetric residue, selecting from $[-H .. H]$. For each integer z :

a: The (symmetric) residue $\langle z^H \rangle_p$ equals $\left(\frac{z}{p}\right)$. Euler criterion.

b: For x, z integers: $\left(\frac{x}{p}\right) \cdot \left(\frac{z}{p}\right) = \left(\frac{xz}{p}\right)$. I.e, mapping $x \mapsto \left(\frac{x}{p}\right)$ is totally-multiplicative. [I.e, $x \mapsto \left(\frac{x}{p}\right)$ is a semigroup-hom $(\mathbb{Z}_p, \cdot, 1) \rightarrow (\{\pm 1, 0\}, \cdot, 1)$, hence is a group-hom $(\Phi_p, \cdot, 1) \rightarrow (\{\pm 1\}, \cdot, 1)$. This holds also for $p=2$.]

c: Value $-1 \in \text{QR}_p$ IFF p is 4POS, i.e, $\left(\frac{-1}{p}\right) = [-1]^{\frac{p-1}{2}}$.

Courtesy Wilson's Thm, value $r := [H!]$ is a mod- p sqroot of -1. i.e, is a p -RONO,^{♡2} when $p \in 4POS$.

d: The number 2 is a p -QR IFF p is 8NEAR, that is, $p \equiv_8 \pm 1$. I.e, $\left(\frac{2}{p}\right) = [-1]^{\frac{p^2-1}{8}}$. ◇

BTWay, the analog of (7a), for Jacobi symbols, does not hold with p replaced by a general odd posint D . E.g, set $D := 9$; so $H = \frac{9-1}{2} = 4$. Setting $z := 2$, then, we have that

$$\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{3}\right) = 1.$$

But $z^H = 2^4 = 16$, whose mod-9 symm-residue isn't even in $\{\pm 1\}$, since $16 \equiv_9 -2$.

^{♡2}RONO is "(square-)Root Of Negative-One".

§Index, with symbols and abbrevs at the End

4POS, 4NEG, 8NEAR, 8FAR, 3

associates, 1

Euler criterion, 3

Euler phi, 1

irreducible element, 1

Legendre-symbol, 3

prime element, 1

unit, 1

zero-divisor, 1

Filename: Problems/Nota/nota.prime-irred.latex
As of: Friday 27Jul2018. Typeset: 27Jul2018 at 22:27.