Partial Theorem List (preliminary)

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/

20 April, 2022 (at *22:43*)

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. Less easily, when $K \perp N$, then $\varphi(KN) = \varphi(K)\cdot\varphi(N)$

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

Divisibility. Use $\equiv_N$ to mean "congruent mod N". Let $n \perp k$ mean that n and k are co-prime [no prime in common].

Use $k \bullet\!| \, n$ for "k divides n". Its negation $k \not\bullet\!| \, n$ means "k does not divide n." Use $n \,|\!\bullet k$ and $n \,|\!\not\bullet k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $p^E \bullet\!\| \, n$, 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.

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: $$Bs + Ct = G.$$

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

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

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: $$s_k := s_0 + k \cdot \frac{C}{G}, \quad t_k := t_0 - k \cdot \frac{B}{G}.$$ ♢

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, written as u^{-1}, is called the ***reciprocal*** [or ***multiplicative-inverse***] of u. [When an elt *has* a mult-inverse, this mult-inverse is unique.]

Exer 1a: If α divides a unit, $\alpha \bullet\!| \, u$, then α is a unit.

Exer 1b: If $\gamma \,|\!\bullet z$ with $z \in$ ZD, then γ is a zero-divisor.

Exer 2: In an arbitrary ring Γ, the set ZD(Γ) is *disjoint* from Units(Γ).

An element $p \in \Gamma$ is:

i: Γ-***irreducible*** if p is a non-unit, non-ZD, such that for each Γ-factorization $p = x \cdot y$, either x or y is a Γ-unit. [Restating, using the definition below: Either $x \approx 1, y \approx p$, or $x \approx p, y \approx 1$.]

ii: Γ-***prime*** if p is a non-unit, non-ZD, such that for each pair $c,d \in \Gamma$: If $p \bullet\!| \, [c \cdot d]$ then *either* $p \bullet\!| \, c$ or $p \bullet\!| \, d$.

Associates. In a *commutative* ring, els α and β are ***associates***, written $\alpha \approx \beta$, if *there exists* a unit u st. $\beta = u\alpha$. [For emphasis, we might say ***strong associates***.] They are ***weak-associates***, written $\alpha \sim \beta$, if $\alpha \bullet\!| \, \beta$ *and* $\alpha \,|\!\bullet \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$].

Ex 3: Prove *Assoc* $\Rightarrow$ *weak-Assoc*.

Ex 4: If $\alpha \sim \beta$ and $\alpha \notin$ ZD, then α, β are (strong) associates.

Ex 5: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* weak-associates. [This, since $2 \cdot 2 \equiv 4$ and $4 \cdot 3 = 12 \equiv 2$.] Are $2, 4$ (strong) associates?

Ex 6: With $d \bullet\!| \, \alpha$, 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 $\boldsymbol{\alpha}$ is irreducible.* ♢

Proof. Consider factorization $\boldsymbol{\alpha} = xy$. Since $\boldsymbol{\alpha} \bullet\!| \, xy$, WLOG $\boldsymbol{\alpha} \bullet\!| \, x$, i.e $\exists c$ with $\boldsymbol{\alpha} c = x$. Hence

$*$: $$\boldsymbol{\alpha} = xy = \boldsymbol{\alpha} cy.$$

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

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 $[x-1][x+1]$.

3: Lemma. *Suppose commRing Γ satisfies the Bézout condition, that each GCD is a linear-combination. Then each irreducible $\boldsymbol{\alpha}$ is prime.* ♢

Pf. Suppose $\boldsymbol{\alpha} \bullet\!| \; c{\cdot}d$. WLOG $\boldsymbol{\alpha} \nmid c$. Let $g := \mathrm{GCD}(\boldsymbol{\alpha}, c)$. Were $g \approx \boldsymbol{\alpha}$, then $\boldsymbol{\alpha} \bullet\!| \; g \bullet\!| \; c$, a contradiction. Thus, since $\boldsymbol{\alpha}$ is irreducible, our $g \approx 1$.

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

$$1 = S\boldsymbol{\alpha} + Tc. \quad \textit{Hence}$$

$$*: \qquad d = S\boldsymbol{\alpha}d + Tcd = Sd\boldsymbol{\alpha} + Tcd.$$

By hyp, $\boldsymbol{\alpha} \bullet\!| \; cd$, hence $\boldsymbol{\alpha}$ divides RhS($*$). So $\boldsymbol{\alpha} \bullet\!| \; d$. ♦

4: Lemma. *In commRing Γ, if prime p divides a project $\alpha_1 \cdots \alpha_K$ then $p \bullet\!| \; \alpha_j$ for some j.* [Exer. 7] ♢

5: Prime-uniqueness thm. *In commRing Γ, suppose*

$$p_1{\cdot}p_2{\cdot}p_3 \cdots p_K = q_1{\cdot}q_2{\cdot}q_3 \cdots q_L$$

are equal products-of-primes. Then $L = K$ and, after permuting the p primes, each $p_k \approx q_k$. ♢

Pf. [From Ex.4, previously, for non-ZD, relations $\sim$ and $\approx$ are the same.] For notational simplicity, we do this in $\mathbb{Z}_+$, in which case $p_k \approx q_k$ will be replaced by $p_k = q_k$.

FTSOC, consider a CEX which minimizes sum $K{+}L$; necessarily positive. WLOG $L{\geq}1$. Thus $K{\geq}1$. [Otherwise, q_L divides a unit, forcing q_L to be a unit; see Ex.1a.] By the preceding lemma, q_L divides *some* p_k; WLOG $q_L \bullet\!| \; p_K$. Thus $q_L = p_K$ [since p_K is prime and q_L is not a unit]. Cancelling now gives $p_1{\cdot}p_2 \cdots p_{K-1} = q_1{\cdot}q_2 \cdots q_{L-1}$, giving a CEX with a *smaller* $[K{-}1] + [L{-}1]$ sum. ♦

Example where $\sim \neq \approx$. Here a modification of an example due to Irving ("Kap") Kaplansky.

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

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

And for $t \leq 0$ define

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

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

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

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 $[-2, 2] \smallsetminus \{0\}$. Cty of g then forces $g \equiv \mathbf{0}$.]

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

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

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

Addendum. By Ex.4, both $\mathcal{E}$ and $\mathcal{D}$ must be zero-divisors. [Exer.8: Exhibit a function $g{\in}\Omega$, *not* the zero-fnc, such that $\mathcal{E}{\cdot}g \equiv \mathbf{0}$.] □

Thus none of the four linear terms is prime. Yet each is Γ-irreducible. (Why?) This ring Γ has zero-divisors (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred$\not\Rightarrow$Prime.

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.

6: Lemma. *In $\mathbb{Z}$, each irreducible element p is necessarily prime.* ♢

Pf. With $p \bullet\!| \; c \cdot d$, 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 $c \,|\!\bullet\, p$. ♦

7a: Fermat's Little Thm (FLiT). *For p prime and each $\mathbf{b} \in \mathbb{Z}$:*

$$\mathbf{b}^p \;\equiv_p\; \mathbf{b}\,.$$ ♢

7b: Euler-Fermat Thm (EFT). *For $N \in \mathbb{Z}_+$ and $\mathbf{b} \perp N$,*

$$\mathbf{b}^{\varphi(N)} \;\equiv_N\; 1\,.$$ ♢

Proof. Define $f\colon \Phi_N \to \Phi_N$ 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

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

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

ASIDE. Alternatively, EFT follows from Lagrange's thm that the order of a subgroup divides the order of the enclosing group. □

a With $N := 19$, then $\varphi(N)=$ ______. Thus EFT (Euler-Fermat) says that $9^{3632} \equiv_N$ ________ $\in [0..N)$.

Soln: Ok, but slow:

```
% (repeated-squaring 9 3632 19 :symmod t)

 /--------------------- Mod 19 ----\
  n:      2^n |     Accum |   9^[2^n]
---+----------+-----------+-------------
  0:        1 |         1 |          9
  1:        2 |         1 |          5
  2:        4 |         1 |          6
  3:        8 |         1 |         -2
  4:       16 |         1 |          4 <<
  5:       32 |         4 |         -3 <<
  6:       64 |         7 |          9
  7:      128 |         7 |          5
  8:      256 |         7 |          6
  9:      512 |         7 |         -2 <<
 10:     1024 |         5 |          4 <<
 11:     2048 |         1 |         -3 <<
All:     done |        -3 |
 \--------------------- Mod 19 ----/

  So  9^{3632}  is mod-19 congruent to the
product of the << marked values, which is -3.
```

What do we learn from a repeated pattern in the $9^{[2^N]}$ column?

Since $\varphi(19) = 18$, faster is

```
& (mod 3632 18)   ->  14
& (repeated-squaring 9 14 19)

 /--------------------- Mod 19 ----\
  n:      2^n |     Accum |   9^[2^n]
---+----------+-----------+-------------
  0:        1 |         1 |          9
  1:        2 |         1 |          5 <<
  2:        4 |         5 |          6 <<
  3:        8 |        -8 |         -2 <<
All:     done |        -3 |
 \--------------------- Mod 19 ----/

  So  9^{14}  is mod-19 congruent to the
product of the << marked values, which is -3.
```

Alternatively. $3632 \equiv_{18} 14 \equiv_{18} -4$. And $\langle 1/9\rangle_{19} = -2$. Thus $\langle 9^{-4}\rangle_{19} = \langle [-2]^4\rangle_{19}$. And indeed…

```
% (repeated-squaring -2 4 19)

 /---------------------- Mod 19 ----\
  n:      2^n |     Accum | [-2]^[2^n]
---+----------+-----------+-----------
  0:        1 |         1 |       -2
  1:        2 |         1 |        4
  2:        4 |         1 |       -3 <<
All:     done |        -3 |
 \--------------------- Mod 19 ----/

  So  [-2]^4  is mod-19 congruent to the
product of the << marked values, which is -3.
```

b $N := \varphi(100) =$ 40 . So $\varphi(N) =$ 16 .
EFT says that $3^{1621} \equiv_N$ ____ $\in [0 .. N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are ____.

Soln: $1621 \equiv_{16} 5$. So $3^5 = 81 \cdot 3 \equiv_{40} 1 \cdot 3 = 3$. Since $3 \perp 40$, EFT applies to tell us $3^{1621} \equiv_{40} 3$. And as $7 \perp 100$, EFT gives $7^{[3^{1621}]} \equiv_{100} 7^3 = 343 \equiv_{100} 43$.

8: Wilson's Thm. *Fix a prime* p. *Then* $\prod(\Phi p) = -1$ *in* $\mathbb{Z}_p$. *Alternatively* $[p-1]! \equiv_p -1$. ◊

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 $125 = 100 + 25 = 10^2 + 5^2$; 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* $8 \perp 51$. *OTOHand,* $-1 \in \text{NQR}_{51}$; *none of the* $\mathbb{Z}_{51}$-*units square to* -1. *Value* 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

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

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 $z \bullet p$.

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 $k \equiv_8 \pm 3$. □

9: 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 $(\mathbb{Z}_p, \cdot, 1) \to (\{\pm 1, 0\}, \cdot, 1)$, hence is a group-hom $(\Phi_p, \cdot, 1) \to (\{\pm 1\}, \cdot, 1)$. 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 (9a), 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

Filename: `Problems/Nota/nota.prime-irred.latex`
As of: *Friday 27Jul2018.* Typeset: *20Apr2022* at *22:43.*