Partial Theorem List (preliminary)

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
28 July, 2016 (at *21:38*)

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

Divisibility. Use $\equiv_N$ to mean "congruent mod N". Let $n \perp k$ mean that n and k are co-prime. Use $k \bullet\!| n$ for "k divides n". Its negation $k \not\bullet\!| n$ means "k does not divide n." Use $n \mid\!\bullet k$ and $n \not\mid\!\bullet k$ 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 $G := \mathrm{Gcd}(B, C)$. 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: $$\sum_{\ell=1}^K B_\ell \cdot s_\ell \;=\; \mathrm{Gcd}(B_1, \ldots, B_K)\,.$$

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: $$\begin{aligned} s_k &:= s_0 + k \cdot \tfrac{C}{G}\,, \\ t_k &:= t_0 - k \cdot \tfrac{B}{G}\,. \end{aligned}$$ ◊

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

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.

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

Two ring-elements α and β are ***associates***, written $\alpha \overset{\text{as}}{\sim} \beta$, if $\alpha \bullet\!| \beta$ *and* $\alpha \mid\!\bullet\, \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$]. They are ***strong associates*** if there exists a unit u st. $\beta = u\alpha$. Exer: Prove *Strong-Assoc ⇒ Assoc.*

Exer: Ring $\mathbb{Z}_N$ has no irreducible elements, since $\mathbb{Z}_N$ is the disjoint-union ZD ⊔ Units.

Exer: PRIME⇒IRRED. However there are rings[♡1] with irreducible elements p which are nonetheless not prime.

Examples. Every ring has the "trivial zero-divisor" —zero itself. The ring of integers doesn't have others. In contrast, the non-trivial zero-divisors of $\mathbb{Z}_{12}$ comprise $\{\pm2, \pm3, \pm4, 6\}$.

In $\mathbb{Z}$ the units are ±1. But in $\mathbb{Z}_{12}$, the ring of integers mod-12, the set of units, $\Phi(12)$, is $\{\pm1, \pm5\}$. In the ring $\mathbb{Q}$ of rationals, *each* non-zero element is a unit. In the ring $\mathbb{G} := \mathbb{Z} + \boldsymbol{i}\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm1, \pm\boldsymbol{i}\}$. [Aside: Units($\mathbb{G}$) is cyclic, generated by $\boldsymbol{i}$. And Units($\mathbb{Z}_{12}$) is not cyclic. For which N is $\Phi(N)$ cyclic?] □

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.

[♡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 (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred≠Prime.

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

Pf. With $p \nmid c\cdot d$, 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 $c \nmid p$. ♦

3a: Fermat's Little Thm (FLiT). *For p prime and each $\mathbf{b} \in \mathbb{Z}$:*

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

3b: Euler-Fermat Thm (EFT). *For $N \in \mathbb{Z}_+$ and $\mathbf{b} \perp N$,*

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

Proof. Define $f{:}\Phi_N{\to}\Phi_N$ 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

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

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

4: 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-*N*QR [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

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

By defn, $(\frac{z}{p})$ is +1, if $z \in \mathrm{QR}_p$; is −1, if $z \in \mathrm{NQR}_p$; and is 0, if $z \not\perp p$, i.e $z \mid\!\bullet\, p$.

An odd integer k is **"4Pos"** if $k \equiv_4 +1$; is 4**Neg** if $k \equiv_4 -1$; is 8**Near** if $k \equiv_8 \pm 1$ (either); is 8**Far** if $k \equiv_8 \pm 3$. □

5: 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: *For x and z integers:* $\left(\frac{x}{p}\right)\cdot\left(\frac{z}{p}\right) = \left(\frac{xz}{p}\right)$. *I.e, the mapping $x \mapsto (\frac{x}{p})$ is totally-multiplicative.* [*I.e, $x \mapsto (\frac{x}{p})$ is a group-hom $(\Phi_p, \cdot, 1) \to (\{\pm1\}, \cdot, 1)$; and this part holds also for p=2.*]

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

c: *Value $-1 \in \mathrm{QR}_p$ 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, 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 (5b), 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 $\{\pm1\}$, since $16 \equiv_9 -2$.

Filename: `Problems/NumberTheory/nt-review.latex`
As of: *Wednesday 30Sep2009.* Typeset: *28Jul2016 at 21:38.*