A special case of Dirichlet's theorem

Jonathan L.F. King
squash@ufl.edu
16 October, 2020 (at *09:18*)

Entrance. An ***arithmetic progression*** (A.P.) means a set $T+M\mathbb{Z}$ of integers,[♡1] where the ***gap*** (or ***modulus***) M is a posint and ***translation*** (or ***target***) T is an integer. I'll also use ***comb*** for "arithmetic progression".

An A.P. $\mathcal{C} := T + M\mathbb{Z}$ is ***coprime*** if $T \perp M$.

1: Dirichlet's Theorem. *Each coprime arithmetic progression contains infinitely many prime numbers.* ♢

While this is difficult to prove in general, there are three easy special[♡2] cases, the combs

$$-1+3\mathbb{Z} \quad -1+4\mathbb{Z} \quad \text{and} \quad -1+6\mathbb{Z}\,.$$

We will establish this last case.

Henceforth, let $\equiv$ mean $\equiv_6$ and let "congruent" mean "mod-6 congruent".

2a: Lemma. *Suppose a product $q_1{\cdot}q_2{\cdot}\ldots{\cdot}q_\ell{\cdot}\ldots{\cdot}q_L$ of integers[♡3] is coprime to 6. Then each multiplicand q_ℓ is coprime to 6.* ♢

Proof. Exer: ; prove the contrapositive. Where does your argument use that each q_ℓ is is an *integer*?

Does the lemma generalize to "6" being replaced by N, an arbitrary posint? ♦

Henceforth, symbols r and q, with or without appendages, range over the integers.

2b: Corollary. *Suppose product $r := q_1{\cdot}q_2{\cdot}\ldots{\cdot}q_L$ is congruent to -1. For oddly-many indices ℓ in $[1\,..\,L]$, then, $q_\ell \equiv -1$.*

In particular, there exists an index $k \in [1\,..\,L]$ such that $q_k \equiv -1$. ♢

Proof. Since $r \perp 6$ (i.e, $-1 \perp 6$), our Lemma tells us that each q_ℓ is coprime to 6. But of the six residue classes $0, \pm1, \pm2, 3$, only[♡2] $+1$ and -1 are coprime to 6. So each q_ℓ is congruent to either $+1$ or -1.

Let D denote the number of indices ℓ st. $q_\ell \equiv -1$. Then

$$r \quad \equiv \quad [-1]^D \cdot [+1]^{L-D} \quad \overset{\text{note}}{=\!=} \quad [-1]^D\,.$$

Consequently, D is odd. ♦

3: Six Theorem. *Comb $\mathcal{C} := -1+6\mathbb{Z}$ owns infinitely many primes.* ♢

Remark. We *could* start our argument by "*FTSOContradiction, suppose $p_1<p_2<\ldots<p_J$ is the complete list of primes in $\mathcal{C}$.*" But instead, let's use the idea for a *constructive argument* that produces new primes from old. To this end, as an alternative to saying "in $\mathcal{C}$", we define an ADJECTIVE: *An integer n is* ***6Neg*** *if $n \equiv_6 -1$, and is* **6Pos** *if $n \equiv_6 +1$.* □

4: The Six Algorithm. *Suppose $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_J$ is a list of* 6Neg *primes. Let $N := \prod_{j=1}^{J} p_j$. Define*

$$\text{4a:} \quad K := \left\{ \begin{matrix} N+4\,, & \text{if } J \text{ is even (i.e } N \equiv +1) \\ N+6\,, & \text{if } J \text{ is odd (i.e } N \equiv -1) \end{matrix} \right\}.$$

Then oddly-many of the prime factors of K are 6Neg*, and none of them is in the given list. Have the algorithm return the least* 6Neg *prime factor.* ♢

Pf that (4) works. The minimum value of N is 1; this, when the list is empty. Thus $K \geqslant 4$, hence is a posint, so we can factor it into a product of primes,

$$*: \qquad K \quad = \quad q_1 \cdot q_2 \cdot \ldots \cdot q_L\,.$$

By its defn, K is 6Neg. Hence Coro. (2b) applies to tell us that oddly many of RhS$(*)$ are 6Neg primes.

The last step is to show that the primes of RhS$(*)$ are new. FTSOC, suppose some q is in $(p_j)_{j=1}^{J}$. Then this q divides both K and N, hence $q \nmid [K-N]$. Thus q divides either 4 or 6, so $q \in \{2,3\}$. But 2 is neither 6Neg nor 6Pos, and ditto for 3; so this contradicts Corollary (2b). Thus no q is in our p-list. ♦

Application. Let $\mathcal{P}$ be $(p_j)_{j=1}^{J}$. When $\mathcal{P}$ is the empty tuple, then $N = 1$ so $K = 1+4 = 5$. Oddly many of the prime factors of 5 are 6Neg; our alg produces the least such, which is 5.

Now set $\mathcal{P} := (5)$. So $N = 5$ and $K = 5+6 = 11$; this produces 11.

Let $\mathcal{P} := (5,5)$. So N=25 and K=29, yielding 29.

Let $\mathcal{P} := (5,11)$; so N=55 and K=59, yielding 59.

[♡1] This is the set $\{T + Mk \mid k \in \mathbb{Z}\}$. Equivalently, it is the set of integers n such that $n \equiv_M T$.

[♡2] No mystery here: The three moduli M=3,4,6 are those with $\varphi(M)$=2. (Euler phi.) The two coprime residue-classes are ±1.

[♡3] If we allow the $\{q_\ell\}_\ell$ to be general real numbers then the result is either false or broken, depending on how you interprete "coprime" for real numbers.

Let $\mathcal{P} := (5, 11, 11)$; so N=605, $J = 3$ and K=611. Now $611 = 13 \cdot 47$, a 6POS times a 6NEG (so oddly many 6NEG, as predicted). Hence the algorithm produces 47.

Lastly, let $\mathcal{P} := (5, 7)$; so N=35, $J = 2$ and K=39. Now $39 = 3 \cdot 13$ and –whoa Nellie!– *neither* of this primes is 6NEG! *What went wrong?* Oh!, *are we a Dufus!* We forgot to check the *hypotheses*! Each prime in $\mathcal{P}$ is supposed to be 6NEG, but 7 is *not* 6NEG. □

Variant. Notice that we can replace (4a) by

4b: $$K := \begin{Bmatrix} N-2\,, & \text{if } J \text{ is even } (\text{i.e } N \equiv +1) \\ N-6\,, & \text{if } J \text{ is odd } (\text{i.e } N \equiv -1) \end{Bmatrix}$$

as long as K is positive. Indeed, the 2 can be replaced by any $\alpha \equiv 2$ *as long as* none of the primes in $\mathcal{P}$ divides α, and K ends up positive. And 6 can be replaced by any $\beta \equiv 0$ with the same restrictions.

Let $\mathcal{P} := (5, 11, 17)$; so N=935 and $J = 3$, so we need a $\beta \equiv 0$ coprime to N. Well, β:=36 is acceptable, yielding 935−36=899, which factors as $29 \cdot 31$. And indeed, oddly many are 6NEG; our routine returns 29, a new 6NEG prime. □

4c: *Variant.* Given a list $\mathcal{P}'$ of 6NEG primes, here is a different replacement for (4a), . To make a new list $\mathcal{P}$ with evenly many members, adjoin to $\mathcal{P}'$, if necessary, a copy of 5. Now set $K := N - 2$. Etc. □

Efficient? The routine would be reasonable *except* for the factor-K-into-primes step. As of Sept2009, no one knows how to factor efficiently. □

Filename: `Problems/NumberTheory/dirichlet-thm.6neg-case.latex`
As of: *Friday 02Oct2009.* Typeset: *16Oct2020* at *09:18.*