An Infinity of Proofs for the Infinity of Primes

Alexander Kovačec, Dep. Math. Univ. Coimbra, 3001-454 Coimbra, Portugal. kovacec@mat.uc.pt

Introductory courses in number theory frequently include as exercises the surprising results on Fermat- and Mersenne primes along with considerations concerning divisors of integers of the form $a^k \pm 1$, see [1, p.] and [2, p. 16].

It seems though that the following two theorems that give a complete discussion of the possible values of $\gcd(a^k \pm 1, a^l \pm 1)$, permit to put these exercises in a more general setting and will make appear them less of isolated, if beautiful, gems. Theorem 1 states the aesthetically pleasing result that for any integer $a \geq 2$ the set $\{1, 2, a+1, a-1, a^2-1, a^2+1, \ldots\}$ is closed with respect to taking greatest common divisors; its proof comprises the first part of that of theorem 2 and it is notable that it does not use any polynomial identities. Some generalizations of the exercises referred are immediate consequences of theorem 2.

Theorem 1 Given an integer $a \geq 2$, any two numbers selected from the set $\mathcal{A} = \{1, 2, a-1, a+1, a^2-1, a^2+1, a^3-1, a^3+1, \ldots\}$ have their greatest common divisor again in $\mathcal{A}$.

A more precise statement implying the above, is the following:

Theorem 2 Given integers $k, l \geq 1$ and $a \geq 2$, and signs $\varepsilon, \delta \in \{\pm 1\}$ there holds with $d = \gcd(k, l)$ the following:

$$\gcd(a^k+\varepsilon, a^l+\delta) = \begin{cases} a^d+1 & \text{iff } \varepsilon = -(-1)^{k/d}, \delta = -(-1)^{l/d}. \\ a^d-1 & \text{if } \varepsilon = \delta = -1 \\ a^d-1 & \text{if } (\varepsilon \neq \delta, \frac{k}{d} \equiv \frac{l}{d} \bmod 2) \wedge (d \geq 2 \vee a \geq 3). \\ 2 \text{ or } 1 & \text{in all other cases according to if } a \text{ is odd or even.} \end{cases}$$

Proof. Consider the following algorithm to be fed with the pairs (k, l) and $(a^k+\varepsilon, a^l+\delta)$.

while $(k, l) \in \mathbb{Z}^2_{\geq 1}$
  if $k \geq l$ **then** replace (k, l) by $(k-l, l)$, and $(a^k+\varepsilon, a^l+\delta)$ by $(a^{k-l}-\delta\varepsilon, a^l+\delta)$ **endif**
  if $k < l$ **then** replace (k, l) by $(l, l-k)$, and $(a^k+\varepsilon, a^l+\delta)$ by $(a^k+\varepsilon, a^{l-k}-\delta\varepsilon)$ **endif**
endwhile

Each execution of the while-loop, makes of the pair (k, l) of exponents a new pair $(k', l') \in \mathbb{Z}^2_{\geq 0}$ satisfying $(k', l') < (k, l)$ in componentwise order. It follows that the algorithm terminates having in line 1 a pair of the form $(0, d)$ or $(d, 0)$ with $d \in \mathbb{Z}_{\geq 1}$. By virtue of the fact that $\gcd(k, l) = \gcd(k-l, l) = \gcd(l, l-k)$ it follows that the gcd of the numbers k, l at the entrance to the while loop will not change. Hence $d = \gcd(k, l)$ and, upon exiting, we find the input pair $(a^k+\varepsilon, a^l+\delta)$ transformed into a pair of the form $(a^0+\varepsilon', a^d+\varepsilon'') = (1+v e', a^d+\varepsilon'')$ or $(a^d+\varepsilon', a^0+\varepsilon'') = (a^d+\varepsilon', 1+\varepsilon'')$, Now, assuming $k \geq l$, the calculation

$$\begin{aligned} \gcd(a^k+\varepsilon, a^l+\delta) &= \gcd(a^k+\varepsilon-a^{k-l}(a^l+\delta), a^l+\delta) \\ &= \gcd(-\delta a^{k-l}+\varepsilon, a^l+\delta) \\ &= \gcd(a^{k-l}-\varepsilon\delta, a^l+\delta) \end{aligned}$$

and a similar calculation for the case $k < l$ yields that the gcds of the pairs of form $(a^k..., ...)$ occuring in lines 2,3 do not change. We conclude, $\gcd(a^k+\varepsilon, a^l+\delta) = \gcd(a^d+\varepsilon', 1+\varepsilon'')$, for some $\varepsilon', \varepsilon'' \in \{\pm 1\}$. Since $1+\varepsilon'' \in \{0, 2\}$ we find $*$: for all admissible $a, k, l, \varepsilon, \delta$, there holds $g := \gcd(a^k+\varepsilon, a^l+\delta) \in \{1, 2, a^d-1, a^d+1\}$.

This is a strengthened version of theorem 1; to prove the refinement we show the following claim.

Claim. Given positive integers d, t with $d|t$ and a sign ε', there holds
a. $a^d+1 | a^t+\varepsilon'$ iff $\varepsilon' = -(-1)^{t/d}$.
b. $a^d-1 | a^t+\varepsilon'$ iff $(\varepsilon' = -1) \vee (d = 1, a = 2) \vee (d = 1, a = 3)$.

$\triangleright$ a. $\Leftarrow$: $a^t+\varepsilon'=(a^d)^{t/d}-(-1)^{t/d}$. Putting $x=a^d$ and $\ell=t/d$ in the identity $x^\ell-(-1)^\ell=(x+1)(x^{\ell-1}-x^{\ell-2}+x^{\ell-3}-x^{\ell-4}+\ldots+(-1)^{\ell-1})$, valid for all $\ell\geq 1$, we find that $a^t+\varepsilon'$ is divisible by a^d+1. $\Rightarrow$: By hypothesis there exists an integer m so that $(a^d)^{t/d}+\varepsilon'=m(a^d+1)$. Putting $u=a^d+1$ we find $(u-1)^{t/d}+\varepsilon'=mu$. Since $u\geq 3$, the binomial theorem implies $(-1)^{t/d}+\varepsilon'=0$.

b. $\Leftarrow$: If the second or third part of the hypothesis hold, the divisibility claimed is clear. Now assume $\varepsilon'=-1$. Then $a^t+\varepsilon'=(a^d)^{t/d}-1$. Putting $x=a^d$ and $\ell=t/d$ in the identity $x^\ell-1=(x-1)(x^{\ell-1}+x^{\ell-2}+\ldots+1)$, valid for all $\ell\geq 1$, we find that $a^t+\varepsilon'$ is divisible by a^d-1. $\Rightarrow$: By hypothesis $(a^d)^{t/d}+\varepsilon'=m(a^d-1)$ for some integer m. Put $u=a^d-1$. Then $(u+1)^{t/d}+\varepsilon'=mu$ The binomial theorem now implies $u|(1+\varepsilon')$. Therefore $\varepsilon'=-1$ or $u\in\{1,2\}$. But the latter holds if and only if second or third part of the conclusion hold true. $\triangleleft$

We can now continue the proof. Because of $d=\gcd(k,l)$ we have only these two possibilities $**$: $\frac{k}{d}\not\equiv\frac{l}{d}$ or $\frac{k}{d}\equiv 1\equiv\frac{l}{d}$. Here and below $\equiv$ stands for congruence $\mod 2$.

The statement concerning g splits into four lines or cases whose justification we give as follows:

Case 1. $\varepsilon=-(-1)^{k/d},\delta=-(-1)^{l/d}$. That this is a necessary and sufficient condition for that $g=a^d+1$ is a direct consequence of $*$ and claim a.

Case 2. $\varepsilon=\delta=-1$. Then $\varepsilon=-(-1)^{k/d},\delta=-(-1)^{l/d}$, cannot hold, for then $k/d\equiv l/d\equiv 0$ which is excluded by $**$. Hence by line 1 and $*$, $g\in\{1,2,a^d-1\}$. Claim b guarantees that a^d-1 is a common divisor of $a^k+\varepsilon, a^l+\delta$. Subcase $(d\geq 2\vee a\geq 3)$: then $a^d-1\geq 2$ and from $*$ it follows that $g=a^d-1$. Subcase $\neg(d\geq 2\vee a\geq 3)$: then $d=1,a=2$. Since $2^k+\varepsilon$ is odd, and $g\neq 2$. Hence $g=1=2^d-1$.

Case 3. $\varepsilon\neq\delta$, $\frac{k}{d}\equiv\frac{l}{d}$. Then evidently line 1 is excluded. So $g\in\{1,2,a^d-1\}$. We can assume $\varepsilon=-1,\delta=+1$, i.o.w. $g=\gcd(a^k-1,a^l+1)$. Now $a^d-1|a^l+1$ by claim a since $1=-(-1)^{l/d}$ using $**$. Also $a^d-1|a^k-1$ by claim b. Subcase $(d\geq 2\vee a\geq 3)$: then $a^d-1\geq 2$, so $g=a^d-1$. Subcase $\neg(d\geq 2\vee a\geq 3)$: then $d=1,a=2$, and since $2^k+\varepsilon$ is odd, we have $g=1=2^d-1$.

Case 4.1. $\varepsilon=\delta=1$, $\frac{k}{d}\not\equiv\frac{l}{d}$. Then we are not in line 1, so $g\in\{1,2,a^d-1\}$. If $g=a^d-1$, then claim b tells us $d=1,a\in\{2,3\}$. But this says that $a^d-1\in\{1,2\}$. So in any case $g\in\{1,2\}$. With only these two possibilities left, we have indeed $g=2$ or 1 corresponding to $a\equiv 1$ or 0.

Case 4.2. $\varepsilon=(-1)^{k/d},\delta=(-1)^{l/d}$, $\frac{k}{d}\not\equiv\frac{l}{d}$. Comparing the hypothesis with line 1 yields $g\in\{1,2,a^d-1\}$; we also see $\varepsilon\neq\delta$; so we can assume by symmetry $\varepsilon=1,\delta=-1$. As before, if $g=a^d-1$, then since $a^d-1|a^k+1$, claim b tells us $d=1,a\in\{2,3\}$ and so again $g\in\{1,2\}$, and g will have the values indicated.

Case 4.3. $\varepsilon\neq\delta,k=l$: In this case we want to find $g=\gcd(a^k+1,a^k-1)$. Since $a^k+1-(a^k-1)=2$ we have $g\in\{1,2\}$, and the claimed values follow.

Till here we have shown that case $i.*$ indeed gives the gcd indicated in line i, $i\in\{1,2,3,4\}$. To conclude we have to show that any quintuple $(k,l,a,\varepsilon,\delta)$ admitted by the hypothesis, satisfies one of the cases contemplated in the proof above.

If $k=l,\varepsilon\neq\delta$ we are in case 4.3; if $k=l,\varepsilon=\delta=-1$ in case 2. The combination $k=l,\varepsilon=\delta=+1$ is contained in case 1 because then $k/d=l/d=1$. If $k\neq l,\varepsilon=\delta=-1$ we are in case 2. If $k\neq l,\varepsilon=\delta=+1$ then if $\frac{k}{d}\equiv\frac{l}{d}$, we are in case 1, else we have $\frac{k}{d}\not\equiv\frac{l}{d}$, and are in case 4.1. If $k\neq l,\varepsilon\neq\delta$ then if $\frac{k}{d}\equiv\frac{l}{d}$, we are in case 3, else we have $\frac{k}{d}\not\equiv\frac{l}{d}$ and so will be in cases 1 or 4.2. ∎

We can deduce easily two well known exercises in number theory concerning Fermat- and Mersenne primes, and generalize another one.

Corollary 3 a. Every prime of the form $a^k+1\geq 3$ is of the form $(2n)^{2^m}+1$.
b. Every prime of the form a^k-1 is of the form 2^p-1 with p prime.

Proof. a. Assume $l|k$, $1\leq l<k$. Then $\gcd(a^k+1,a^l+1)=1$. In the notation of theorem 1, $d=l$, $1=\delta=-(-1)^{l/d}$. Since $a^l+1\neq 1$, we must have $\varepsilon=1\neq-(-1)^{k/l}$, that is $k/l\equiv 0$. This holding for

all proper divisors of k, we find that k must be a power of 2 as claimed. Since (ε, δ) does not satisfy the conditions of lines 1,2,3 of theorem 1, a must be even.

b. If $a^k - 1$ is prime, then $\gcd(a^k - 1, a^l - 1) = 1$ for all l satisfying $l|k, 1 \leq l < k$. Since line 2 of theorem 1 applies and $d = l$, we have $a^l - 1 = 1$. This can only hold if $a = 2, l = 1$; i.o.w. $a = 2$ and k is prime. ∎

Recall that one defines for $n \in \mathbb{Z}$ and p prime the order of n at p by $\operatorname{ord}_p(n) := \max\{k : p^k|n\}$.

Corollary 3 Let a be even. Then a^k+1 and a^l+1 are relatively prime if and only if $\operatorname{ord}_2(k) \neq \operatorname{ord}_2(l)$; in particular a sequence $\{a^{k_i} + 1\}_{i=1}^{\infty}$ consists of pairwisely relatively prime integers if and only if the sequence $\{\operatorname{ord}_2(k_i)\}_{i=1}^{\infty}$ consists of pairewisely distinct integers.

Proof. Write $k = 2^{k'}k'', l = 2^{l'}l''$ with k'', l'' odd. Let $d = \gcd(k, l)$. We have $\operatorname{ord}_2(d) = \min\{k', l'\}$. Note that $-(-1)^{k/d} = 1/-1$ according to if $\operatorname{ord}_2(k/d) \ = 0/ > 0$. By theorem 1, $a^k + 1, a^l + 1$ are relatively prime iff $\neg(1 = -(-1)^{k/d} = -(-1)^{l/d})$ iff $\neg(\operatorname{ord}_2(k/d) = \operatorname{ord}_2(l/d) = 0)$ iff $(k' - \min\{k', l'\} \neq 0$ or $l' - \min\{k', l'\} \neq 0)$ iff $l' \neq k'$. ∎

Since each integer is divisible by a prime, it follows that the infinitely many possible choices for a and sequences k_i with pairwise distinct $\operatorname{ord}_2(k_i)$ give different proofs for the infinity of primes. (The fundamental theorem of artithmetic we used to in above decomposition $k = 2^{k'}k''$ etc. does not depend on this infinity.) According to [2, p26c-4] the following result was observed by G. Polya for the case that $b = 2$; it is evidently a consequence of corollary 3.

Corollary 4 Let $a, b \in \mathbb{Z}_{\geq 2}$ be even. Then no two numbers in the sequence $u_k = a^{b^k}+1,\ k = 1, 2, \ldots$ have a common prime divisor. ∎

Corollary 5 Let $a, b \in \mathbb{Z}$, $a \geq 2$, b odd. Then any two numbers in the sequence $u_k = a^{b^k} + 1,\ k = 1, 2, \ldots$ divide each other.

Proof. Given k, l we have with $d = \gcd(b^k, b^l) = b^{\min\{k,l\}}$ that $\{b^k/d, b^l/d\} = \{1, b^{|k-l|}\}$. Both these numbers are odd, hence from theorem 1, $\gcd(u_k, u_l) = \gcd(a^{b^k} + 1, a^{b^l} + 1) = a^{b^{\min\{k,l\}}} + 1 = u_{\min\{k,l\}}$, which proves the claim. ∎

References

[1] I. Niven, I and Zuckerman, H. An Introduction to the Theory of Numbers, J. Wiley 1972.

[2] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, GTM 84, Springer 1982.