Adding Units Mod n

Elem. Math. 55 (2000) 123 – 127
0013-6018/00/030123-5 $ 1.50+0.20/0

Elemente der Mathematik

Adding Units Mod n

Marian Deaconescu

Marian Deaconescu is from Romania, but works now abroad in Kuwait. His main interests in mathematics are related to group theory. His two little daughters, black and white photography, fishing and dog breeding are his reasons for doing much less mathematics than he should.

dedicated to Nicolae Popescu

Fix an integer $n \geq 2$ and denote by $U(Z_n)$ the group of units of the ring Z_n of residue classes modulo n. Thus $U(Z_n) = \{\overline{k} \in Z_n \mid (k, n) = 1\}$. $U(Z_n)$ is not closed with respect to addition; for example, $\overline{1} \in U(Z_2)$, but $\overline{1} + \overline{1} = \overline{0} \notin U(Z_2)$.

If one plays with the *addition* tables for $U(Z_n)$ for a short while, one observes that if n is odd, then *every* element of Z_n appears as a result in the table. Stated in other terms, the equation $\overline{x} + \overline{y} = \overline{k}$ seems to have solutions $\overline{x}, \overline{y} \in U(Z_n)$ for every $\overline{k} \in Z_n$.

If n is even, however, one quickly observes that the odd residue classes are never sums of units in $U(Z_n)$; the reason is plain to see: n being even, the residue classes in $U(Z_n)$ are forced to be odd so the sum of two units is never an odd residue class.

Es ist wohlbekannt, dass für eine Primzahl p die Kongruenz $x + y \equiv 0 \bmod p$ genau p Lösungen hat, welche durch die Paare $(0,0), (1, p-1), \ldots, (p-1, 1)$ repräsentiert werden können. Abgesehen von der trivialen Lösung $(0,0)$ sind die Komponenten der übrigen Lösungen alle von Null verschiedene Restklassen im Körper $\mathbf{F}_p$ mit p Elementen. Dies beweist insbesondere, dass die Anzahl der $\mathbf{F}_p$-rationalen Punkte des 1-dimensionalen projektiven Raumes gleich p ist. Die analoge Fragestellung für Systeme von Polynomen höheren Grades in mehreren Veränderlichen führt zu den Vermutungen von A. Weil, welche in den siebziger Jahren durch P. Deligne gelöst wurden. Im vorliegenden Beitrag beschäftigt sich M. Deaconescu mit folgender Variation der eingangs geschilderten Problemstellung: er beantwortet die Frage nach der Anzahl der zu n teilerfremden Lösungen $x, y \bmod n$ der Kongruenz $x + y \equiv k \bmod n$, wobei k, n beliebige natürliche Zahlen sind. *jk*

∗) While writing this note, the author was supported by K.U.Research Grant SM177.

These elementary remarks suggest the natural problem of finding, given some class $\bar{k} \in Z_n$, how many times does this class $\bar{k}$ appear as a result in the addition table of $U(Z_n)$. In different terminology: fix some integer $n \geq 2$ and for every integer k with $0 \leq k \leq n-1$ determine the number $s(k)$ defined as follows:

$$s(k) = |\{(\bar{x}, \bar{y}) \in U(Z_n) \times U(Z_n) \mid \bar{x} + \bar{y} = \bar{k}\}|.$$

To be sure, this is not quite an obvious exercise. For if one tries constructing the addition tables for $U(Z_n)$ for more and more complicated numbers n (using a computer helps in performing this tedious task), the more and more elusive a working conjecture seems to appear.

The answer to our problem turns out to depend, unexpectedly, on considerations related to the number of fixed points of automorphisms of the additive group $(Z_n, +)$.

Theorem. *Let $n \geq 2$ be an integer, let $0 \leq k \leq n-1$ and let $s(k)$ denote the number of solutions $(\bar{x}, \bar{y}) \in U(Z_n) \times U(Z_n)$ of the equation $\bar{x} + \bar{y} = \bar{k}$. Then*

$$s(k) = \frac{\varphi(n)}{\varphi(n/d)} \Psi(d, n)$$

where $d = (k, n)$ and $\Psi(d, n)$ is the number of those automorphisms of the additive group Z_n having exactly d fixed points.

In the statement of the Theorem, (k, n) stands for the greatest common divisor of k and n, while $\varphi(n)$ is the value at n of Euler's totient function.

Proof. Let α be an automorphism of the additive group Z_n. Then $Fix(\alpha) = \{\bar{k} \in Z_n \mid \alpha(\bar{k}) = \bar{k}\}$ is a subgroup of Z_n and consequently, by Lagrange's theorem, $|Fix(\alpha)|$ is a divisor of n. For a divisor d of n, let $\Psi(d, n)$ denote the number of those automorphisms of the (additive) cyclic group Z_n which have d fixed points.

Observe first that

$$\Psi(d, n) = |\{\bar{u} \in U(Z_n) \mid (u-1, n) = d\}|. \tag{1}$$

In order to prove (1), notice that one can identify every automorphism $\alpha \in Aut(Z_n, +)$ with a fixed unit $\bar{u} \in U(Z_n)$ in such a way that $\alpha(\bar{k}) = \bar{k}\bar{u}$. Therefore $|Fix(\alpha)| = |Fix(\bar{u})| = |\{\bar{k} \in Z_n \mid \bar{k}\bar{u} = \bar{k}\}| = |\{\bar{k} \in Z_n \mid n | k(u-1)\}| = (u-1, n)$. This proves the claim.

Remember that we want to count the number $s(k)$ of solutions in $U(Z_n)$ of the equation

$$\bar{x} + \bar{y} = \bar{k}\,. \tag{$*$}$$

Let $d = (k, n)$, so that $\bar{k} = \bar{d}\bar{t}^{-1}$ for some fixed $\bar{t} \in U(Z_n)$. Transform now $(*)$ into successive (and uglier) forms:

$$\bar{x} + \bar{y} = \bar{d}\bar{t}^{-1} \Leftrightarrow \bar{x}\bar{t} + \bar{y}\bar{t} = \bar{d} \Leftrightarrow \bar{x} + \bar{y} = \bar{d} \Leftrightarrow \bar{x}\bar{y}^{-1} + 1 = \bar{d}\bar{y}^{-1} \Leftrightarrow \bar{x}\bar{y} + \bar{1} = \bar{d}\bar{y} \Leftrightarrow -\bar{x}\bar{y} + \bar{1} = \bar{d}\bar{y}.$$

A word of caution is in place here: when passing from one form of the equation to another, the equivalence sign is used to indicate that both equations have the same number of solutions.

Turning back to the long list of equivalences: the latter equation has the same number of solutions as $(*)$, but it has two advantages. Notice first that $d = (dy, n) = (xy - 1, n)$. Next, observe that as $\overline{y}$ runs over $U(Z_n)$, the expression $d\overline{y}$ takes on exactly $\varphi(n/d)$ distinct values in Z_n. By combining these remarks with formula (1), one sees that $s(k) = \frac{\varphi(n)}{\varphi(n/d)}\Psi(d, n)$, as asserted.

Suppose that one can find the primary decomposition of n (easy to suppose, but usually hard to achieve in practice – a fact that should always be stressed!), i.e. $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ and let $d = \prod_{i=1}^{s} p_i^{\beta_i}$ be a divisor of n. It was determined in [1] that

$$\Psi(d, n) = \prod_{\substack{p_i | n/d \\ p_i | d}} p_i^{\alpha_i - \beta_i - 1}(p_i - 1) \prod_{\substack{p_j | n/d \\ p_j \nmid d}} p_j^{\alpha_j - 1}(p_j - 2). \tag{2}$$

Based on the Theorem and on formula (2), the numbers $s(k)$ can be calculated effectively provided that a primary decomposition of n is at hand. Formula (2) also helps deriving a first immediate consequence of the Theorem:

Corollary 1 *Let $n \geq 2$ be an integer.*

i) *If n is odd, then every element of Z_n is a sum of two units.*

ii) *If n is even, then $\overline{k} \in Z_n$ is a sum of two units if and only if k is even.*

Proof. i) If n is odd, formula (2) indicates that $\Psi(d, n) \neq 0$ for all divisors d of n and the result follows from the Theorem.

ii) By (2) and by the Theorem, $s(k) \neq 0 \Leftrightarrow \Psi(d, n) \neq 0$, where $d = (k, n) \Leftrightarrow d$ is even$\Leftrightarrow k$ is even.

The Theorem has another, less obvious consequence in the realm of positive integers – an inequality which "fingerprints" the primes in its extreme case.

Such inequalities are not at all uncommon. Just consider this one: if $n \geq 2$ is an integer, then $\varphi(n) \leq n - 1$ and the equality occurs if and only if n is a prime. Admittedly, these results are cute, but they have limited practical value and one wonders why to add one more to the already existing collection. Here are some reasons: the following inequality involves a less usual arithmetic function, namely $\Psi(1, n)$, it suggests a natural conjecture which I think is true, but very hard to solve and its proof uses the numbers $s(k)$.

Corollary 2 *Let $n \geq 2$ be an integer and let $\Psi(1, n)$ denote the number of the fixed-point-free automorphisms of the additive group Z_n. Then*

$$\varphi(n)(\varphi(n) - 1) \geq (n - 1)\Psi(1, n)$$

and the equality occurs if and only if n is a prime.

Proof. As the notation $\Psi(1,n)$ suggests, a fixed-point-free automorphism of the additive group Z_n is an automorphism which fixes only the identity class 0.
Take $d = 1$ in formula (2) to obtain

$$\Psi(1,n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 2). \tag{3}$$

Observe next that, by definition of $s(k)$, one obtains:

$$\sum_{k=0}^{n-1} s(k) = \varphi(n)^2. \tag{4}$$

Indeed, $U(Z_n)$ has $\varphi(n)$ elements and its addition table has $\varphi(n)^2$ entries.
Apply the Theorem twice to get:

$$s(0) = \varphi(n) \tag{5}$$

and

$$s(k) = \Psi(1,n) \text{ whenever } (k,n) = 1. \tag{6}$$

Now use (2) and (3) to obtain, after a rather long – but elementary – calculation, that

$$\text{For } n \text{ odd and for } d \text{ a proper divisor of } n,\ \varphi(n)\Psi(d,n) > \varphi(n/d)\Psi(1,n). \tag{7}$$

After this preparation one is ready to prove Corollary 2. Let first $n \geq 4$ be even, so that by (3) $\Psi(1,n) = 0$. The statement is correct in this case.

Suppose next that n is odd and composite; then there exists some k, $0 < k < n-1$ with $(k,n) > 1$ and one obtains:

$$\varphi(n)(\varphi(n) - 1) = \varphi(n)^2 - \varphi(n) = \qquad \text{(by (4) and (5))}$$

$$\sum_{k=1}^{n-1} s(k) = \sum_{(k,n)=1} s(k) + \sum_{(k,n)>1} s(k) = \qquad \text{(by (6))}$$

$$\varphi(n)\Psi(1,n) + \sum_{(k,n)>1} s(k) > \qquad \text{(by (7) and by Theorem)}$$

$$\varphi(n)\Psi(1,n) + (n - 1 - \varphi(n))\Psi(1,n) = (n-1)\Psi(1,n).$$

Finally, let n be a prime. Then (3) gives that $\Psi(1,n) = n - 2$ and since clearly $\varphi(n) = n - 1$ one verifies easily that the equality holds in this case. The proof is complete.

Remark. The inequality in Corollary 2 can be proved directly, by brute force inequalities, but it is a bit odd to do so.

It should be apparent by now that the numbers $\Psi(1,n)$ bear a strong resemblance with $\varphi(n)$: just consider their value if n is a prime or a square-free number. A well-known (and as far as I am aware yet unsolved) conjecture of D.H. Lehmer [3] asserts that if $n \geq 2$ and if $\varphi(n)$ divides $n-1$, then n must be a prime.

By analogy and inspired by Corollary 2, one may conjecture that the integers $n \geq 2$ for which $\Psi(1,n)$ divides $\varphi(n)-1$ must be primes. I expect this conjecture to be as hard as Lehmer's. The reader who wishes to read more about partial results related to Lehmer's conjecture could consult [2] for a partial bibliography.

I want to extend here my thanks to my good friend Vali Filip. A nurse by training and vocation, with the patience of an angel, he was able to understand most of the material, although on occasion I had to explain to him what is a group and an automorphism of it.

References

[1] M. Deaconescu and H.K. Du, *Counting similar automorphisms of finite cyclic groups*, Math. Japonica **46** (1997), 345–348.

[2] R.K. Guy, *Unsolved problems in Number Theory*, Springer Verlag, 1981.

[3] D.H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), 745–751.

Marian Deaconescu
Dept. of Mathematics and Computer Science
Kuwait University
P.O. Box 5969
Safat 13060
Kuwait
e-mail: DEACON@math-1.sci.kuniv.edu.kw