ACTA ARITHMETICA
LXIV.4 (1993)

Generating units modulo an odd integer by addition and subtraction

by

H. W. Lenstra, Jr. (Berkeley, Cal.)

An *addition-subtraction chain* is a finite sequence of integers that begins with 1, and in which every member except the first one is the sum or the difference of two not necessarily different earlier members.

Theorem 1. *Let n be an odd integer, and let a be an integer satisfying* $\gcd(a, n) = 1$. *Then there exists an addition-subtraction chain that ends with a and that consists of integers that are relatively prime to n.*

This theorem is proved below. It answers a question that F. Alberto Grünbaum raised in connection with the phase problem in crystallography.

In principle, one can use our proof of Theorem 1 to obtain an upper bound for the length of the addition-subtraction chain and for the absolute values of its members, but it is not likely to be a very good one.

Let $\mathbb{Z}$ be the ring of integers, and let $n \in \mathbb{Z}$. Denote by $\mathbb{Z}/n\mathbb{Z}$ the ring of integers modulo n. The image of an integer a under the natural map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is denoted by $(a \bmod n)$, or simply by a if there is no ambiguity about n. Let $(\mathbb{Z}/n\mathbb{Z})^*$ be the group of units of $\mathbb{Z}/n\mathbb{Z}$, and let the order of $(\mathbb{Z}/n\mathbb{Z})^*$ be denoted by $\varphi(n)$.

Theorem 2. *Let n be a positive odd integer, and let $H \subset (\mathbb{Z}/n\mathbb{Z})^*$ be a subgroup containing -1 with the property that if $u \in H$ is such that $u - 1 \in (\mathbb{Z}/n\mathbb{Z})^*$, then $u - 1 \in H$. Then $H = (\mathbb{Z}/n\mathbb{Z})^*$.*

We shall first prove Theorem 2. It will be used in the proof of Theorem 1.

If n, H satisfy the conditions of Theorem 2, then we have

(1) if u, $v \in H$ are such that $u + v \in (\mathbb{Z}/n\mathbb{Z})^*$, then $u + v \in H$.

1991 *Mathematics Subject Classification*: 11A07, 11B75.

Key words and phrases: addition-subtraction chain, coprime residue classes.

The author was supported by NSF under Grant No. DMS 90-02939.

To prove this, put $w = -uv^{-1}$. Then $w \in H$ and $w - 1 = -v^{-1}(u + v) \in (\mathbb{Z}/n\mathbb{Z})^*$, so $w - 1 \in H$ and therefore $u + v = -v(w - 1) \in H$. From (1) it follows that

$$2 \in H, \quad 4 \in H. \tag{2}$$

The proof of Theorem 2 depends on the following auxiliary result.

LEMMA. *Let n, H satisfy the conditions of Theorem 2, and let d be a divisor of n. Assume that the following conditions are satisfied:*

(i) $\gcd(d, n/d) = 1$;
(ii) *there exists $u \in H$, $u \neq 1$, with $u \equiv 1 \bmod d$;*
(iii) *for each $u \in H$, $u \neq 1$, with $u \equiv 1 \bmod d$ one has $\gcd(u - 1, n) = d$.*

Then n/d is a prime number, and the number of $u \in H$ with $u \equiv 1 \bmod d$ is $(n/d) - 1$.

In the proof of the lemma we write $e = n/d$. We have $\gcd(d, e) = 1$, so by the Chinese remainder theorem we may identify $\mathbb{Z}/n\mathbb{Z}$ with $(\mathbb{Z}/d\mathbb{Z})\times(\mathbb{Z}/e\mathbb{Z})$; in this identification, $(a \bmod n)$ corresponds to $(a \bmod d, a \bmod e)$, and we have $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/d\mathbb{Z})^* \times (\mathbb{Z}/e\mathbb{Z})^*$. Write

$$I = \{v \in (\mathbb{Z}/e\mathbb{Z})^* : (1, v) \in H\}.$$

This is a subgroup of $(\mathbb{Z}/e\mathbb{Z})^*$, and it is isomorphic to the kernel of the natural map $H \to (\mathbb{Z}/d\mathbb{Z})^*$ that sends u to $(u \bmod d)$. Condition (ii) of the lemma is clearly equivalent to $\#I > 1$, and condition (iii) to

$$v - 1 \in (\mathbb{Z}/e\mathbb{Z})^* \quad \text{for all } v \in I,\ v \neq 1. \tag{3}$$

From $\#I > 1$ it follows that $e > 1$. We claim that

$$\sum_{x\in I} x = 0 \quad (\text{in } \mathbb{Z}/e\mathbb{Z}). \tag{4}$$

To prove this, choose $v \in I$, $v \neq 1$. Then $vI = I$, so

$$(v - 1)\sum_{x\in I} x = \sum_{x\in I} vx - \sum_{x\in I} x = 0.$$

By (3), this implies (4). Next we show that

$$v + 1 \in (\mathbb{Z}/e\mathbb{Z})^* \quad \text{for all } v \in I,\ v \neq -1. \tag{5}$$

Suppose that $v \in I$ is such that $v+1 \notin (\mathbb{Z}/e\mathbb{Z})^*$. Then we have $v \neq 1$. Also, from $v^2 \in I$ and $v^2 - 1 = (v - 1)(v + 1) \notin (\mathbb{Z}/e\mathbb{Z})^*$ it follows by (3) that $v^2 = 1$. Then $(v - 1)(v + 1) = 0$, which by (3) implies that $v + 1 = 0$, so $v = -1$. This proves (5).

Let $v \in I$, $v \neq -1$. Then $(1, v) \in H$ and $(1, v) + (1, 1) = (2, v + 1) \in (\mathbb{Z}/d\mathbb{Z})^* \times (\mathbb{Z}/e\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^*$, so $(2, v + 1) \in H$. By (2), this implies that $(1, (v+1)/2) = (2, v+1)\cdot 2^{-1} \in H$, and therefore $(v+1)/2 \in I$ and $v+1 \in 2I$.

This proves that $I+1 \subset (2I) \cup \{0\}$. The cardinality of $I+1$ is one less than that of $(2I) \cup \{0\}$. We can determine the missing element by comparing the sums of the elements in the two sets. Putting $k = \#I$ we find from (4) that

$$\sum_{x \in I+1} x = k \bmod e, \qquad \sum_{x \in (2I) \cup \{0\}} x = 0\,.$$

Therefore we have

$$(I+1) \cup \{-k \bmod e\} = (2I) \cup \{0\}\,. \tag{6}$$

Comparing the cardinalities of the two sets we see that $(-k \bmod e) \notin I+1$, that is,

$$(-k-1 \bmod e) \notin I\,. \tag{7}$$

Since k is the order of a subgroup of $(\mathbb{Z}/e\mathbb{Z})^*$, we have $1 \le k \le \varphi(e) < e$, so $(-k \bmod e) \neq 0$. Therefore (6) shows that $(-k \bmod e) \in 2I$, so $(1, -k/2) \in H$ and hence $(2, -k) = 2 \cdot (1, -k/2) \in H$. However, from (7) we see that $(2, -k) - 1 = (1, -k-1) \notin H$, so $(1, -k-1) \notin (\mathbb{Z}/n\mathbb{Z})^*$. Therefore we have

$$\gcd(k+1, e) > 1\,. \tag{8}$$

From $(-k \bmod e) \neq 0$ and (6) we find that $0 \in I+1$, that is, $-1 \in I$. Because -1 has order 2 it follows that the order k of I is *even*. From $-I = I$ and (6) we obtain

$$(I-1) \cup \{k \bmod e\} = (2I) \cup \{0\}\,. \tag{9}$$

We deduce that if $1 \le i \le k$, then $(i \bmod e) \in I$ if i is odd and $(i \bmod e) \in 2I$ if i is even. This is proved by induction on i, the case $i = 1$ being obvious. If i is even, $2 \le i \le k$, then by the inductive assumption we have $i-1 \in I$, so $i = (i-1)+1 \in I+1$, and from (6) and $i \neq 0$ one gets $i \in 2I$. If i is odd, $1 < i < k$, then by the inductive assumption we have $i - 1 \in 2I$, and from (9) and $i \neq k+1$ one obtains $i \in I$.

We claim that actually

$$I = \{\pm 1,\, \pm 3,\, \ldots,\, \pm(k-1)\}, \qquad 2I = \{\pm 2,\, \pm 4,\, \ldots, \pm k\}\,.$$

The inclusions $\supset$ follow from what we just proved combined with $-1 \in I$. To show equality it suffices to prove that the k elements of each of the sets on the right are pairwise distinct modulo e; and this follows from the fact that all differences are even and less than $2e$ in absolute value.

Since all elements of I are relatively prime to e, the description of I given above shows that e has no prime divisor less than k. Therefore (8) implies that

$$k+1 \text{ is the least prime divisor of } e.$$

Suppose that e is not a prime number. Then $k < e/2$, so the description of I given above shows that $2 \notin I$. Hence $4 \notin 2I$, which by the description of $2I$ given above implies that $k = 2$. Then the number $k+1 = 3$ divides e, so 3 does not divide d. From (2) and $(1, -1) \in H$ we obtain $(2, -2) \in H$. Since $(2, -2) + 1 = (3, -1) \in (\mathbb{Z}/n\mathbb{Z})^*$ we have $(3, -1) \in H$, so also $(3, 1) = (3, -1) \cdot (1, -1) \in H$. From $(3, 1) + 1 = (4, 2) \in (\mathbb{Z}/n\mathbb{Z})^*$ we get $(4, 2) \in H$, which by $(4, 4) = 4 \in H$ implies that $(1, 2) \in H$. This contradicts the fact that $2 \notin I$.

We conclude that e is a prime number. Then $k + 1 = e$, so we have $\#I = k = e - 1$. This completes the proof of the lemma.

We now prove Theorem 2 by induction on n. The case $n = 1$ is obvious, so let $n > 1$.

Let it first be assumed that n has a repeated prime factor. Let p be a prime number for which p^2 divides n, and write $n = dp^m$, where $d \not\equiv 0 \bmod p$ and $m \geq 2$. Then condition (i) of the lemma is satisfied.

We prove that for any integer l with $1 \leq l \leq m-1$ the image of H under the natural map $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/dp^l\mathbb{Z}$ is the full unit group $(\mathbb{Z}/dp^l\mathbb{Z})^*$. By the induction hypothesis, it suffices for this to check that $-1 \in fH$ and that for any $w \in fH$ with $w - 1 \in (\mathbb{Z}/dp^l\mathbb{Z})^*$ one has $w - 1 \in fH$. The first of these follows from $-1 \in H$ and $f(-1) = -1$. To prove the second, choose $u \in H$ with $w = f(u)$. Then $f(u-1) = w - 1$, so from $w - 1 \in (\mathbb{Z}/dp^l\mathbb{Z})^*$ and the fact that n and dp^l have the same prime factors it follows that $u - 1 \in (\mathbb{Z}/n\mathbb{Z})^*$. Therefore one has $u - 1 \in H$, which leads to the desired conclusion $w - 1 = f(u-1) \in fH$.

Applying what we just proved to $l = 1$ one finds that $\#H \geq \varphi(dp) > \varphi(d)$. Therefore the natural map $g\colon H \to (\mathbb{Z}/d\mathbb{Z})^*$ is not injective, and the kernel of g contains an element $u \neq 1$. This means that condition (ii) of the lemma is satisfied.

The conclusion of the lemma does not hold, since $n/d = p^m$ is not a prime number. Therefore condition (iii) of the lemma is not satisfied, and there exists $u \in H$ with $u \neq 1$, $u \equiv 1 \bmod d$, $\gcd(u-1, n) \neq d$. Then we have $\gcd(u-1, n) = dp^l$ for some integer l with $1 \leq l \leq m-1$, so we can write $u = 1 + drp^l$ for some integer r with $r \not\equiv 0 \bmod p$. It follows that for each non-negative integer i there is an integer r_i with

$$u^{p^i} = 1 + dr_i p^{l+i}, \qquad r_i \not\equiv 0 \bmod p\,.$$

One proves this by induction on i, by means of the binomial theorem. In particular, we see that

$$u^{p^{m-l}} = 1, \qquad u^{p^{m-l-1}} \neq 1 \qquad (\text{in } \mathbb{Z}/dp^m\mathbb{Z} = \mathbb{Z}/n\mathbb{Z})\,,$$

so the order of u equals p^{m-l}.

Now consider the natural map $f\colon H \to (\mathbb{Z}/dp^l\mathbb{Z})^*$. We showed above that f is surjective, so $\#fH = \varphi(dp^l)$. The kernel of f contains u, so

$\#\ker f \geq p^{m-l}$. Hence we have $\#H = \#\ker f \cdot \#fH \geq p^{m-l} \cdot \varphi(dp^l) = \varphi(n)$, and therefore $H = (\mathbb{Z}/n\mathbb{Z})^*$, as required.

Let it next be supposed that n has no repeated prime factor, so that it is squarefree. Let $d = \max\{\gcd(u-1, n) : u \in H,\, u \neq 1\}$; note that this is well-defined, since $-1 \in H$, $-1 \neq 1$. Then conditions (ii) and (iii) of the lemma are clearly satisfied. Condition (i) is also satisfied, since n is squarefree. The lemma now implies that the number n/d, which we denote by e, is a prime number, and that the kernel of the natural map $g\colon H \to (\mathbb{Z}/d\mathbb{Z})^*$ has order $e-1$. We claim that g is surjective. By the induction hypothesis, it suffices for this to check that $-1 \in gH$ and that for any $w \in gH$ with $w - 1 \in (\mathbb{Z}/d\mathbb{Z})^*$ one has $w - 1 \in gH$. The first of these follows from $-1 \in H$ and $g(-1) = -1$. To prove the second, we identify $(\mathbb{Z}/n\mathbb{Z})^*$ with $(\mathbb{Z}/d\mathbb{Z})^* \times (\mathbb{Z}/e\mathbb{Z})^*$, as we did in the proof of the lemma. Then from $\#\ker g = e - 1$ it follows that $\{1\} \times (\mathbb{Z}/e\mathbb{Z})^* \subset H$, and this implies that $H = gH \times (\mathbb{Z}/e\mathbb{Z})^*$. Therefore, if $w \in gH$ then for each $v \in (\mathbb{Z}/e\mathbb{Z})^*$ the element $u = (w, v)$ belongs to H. Choose $v \neq 1$; then $u - 1 \in (\mathbb{Z}/n\mathbb{Z})^*$, so $u - 1 \in H$, which leads to the desired conclusion $w - 1 = g(u-1) \in gH$.

The surjectivity of g implies that $H = gH \times (\mathbb{Z}/e\mathbb{Z})^* = (\mathbb{Z}/d\mathbb{Z})^* \times (\mathbb{Z}/e\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^*$, as required. This completes the proof of Theorem 2.

Theorem 2 admits the following reformulation. Let n be a positive odd integer, and let a subset $S \subset (\mathbb{Z}/n\mathbb{Z})^*$ be called *additively closed* if for any $u, v \in S$ with $u + v \in (\mathbb{Z}/n\mathbb{Z})^*$ one has $u + v \in S$. With this terminology, Theorem 2 implies that *the only additively closed subset of* $(\mathbb{Z}/n\mathbb{Z})^*$ *containing* 1 *and* -1 *is* $(\mathbb{Z}/n\mathbb{Z})^*$ *itself*.

To prove this, denote by H the intersection of all additively closed subsets of $(\mathbb{Z}/n\mathbb{Z})^*$ that contain 1 and -1. It clearly suffices to prove that $H = (\mathbb{Z}/n\mathbb{Z})^*$. Obviously, H itself is additively closed, and so is $-H$. Also, $-H$ contains both -1 and 1, so by definition of H we have $H \subset -H$. It follows that $H = -H$. Next let $u \in H$. Then $u^{-1}H$ is additively closed, and it contains 1 and -1, so we have $H = u^{-1}H$. This implies that H is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. The conditions of Theorem 2 are satisfied, so we find that $H = (\mathbb{Z}/n\mathbb{Z})^*$, as required.

We now prove Theorem 1. Let n be an odd integer, and let the set $T \subset \mathbb{Z}$ consist of all integers a for which an addition-subtraction chain as in the conclusion of the theorem exists. We need to prove that T consists of all integers that are relatively prime to n.

If a, $b \in T$ are such that $\gcd(a+b, n) = 1$, then one clearly has $a+b \in T$, and likewise for $a - b$. By induction on i one finds that $2^i \in T$ for all non-negative integers i. From $1 - 2 = -1$ one obtains $-1 \in T$, and this readily implies that $T = -T$.

Let l be a positive integer for which $2^l \equiv 1 \bmod n$, and put $m = 2^l - 1$. Then m is a positive odd integer, and m is a multiple of n. By induction on i we prove that $im + 1 \in T$ for all non-negative integers i. For $i = 0$ this is clear, so let $i > 0$. Then we have $(i-1)m + 1 \in T$ by the inductive assumption, and from $((i-1)m+1) + 2^l = im + 2$ and $\gcd(im+2, n) = \gcd(2, n) = 1$ it follows that $im + 2 \in T$. By $(im+2) + (-1) = im + 1$, $\gcd(im+1, n) = 1$ this implies that $im + 1 \in T$, as asserted. From $(im + 1) - 2 = im - 1$ we find that also $im - 1 \in T$ for all non-negative integers i. With $T = -T$ it follows that $im \pm 1 \in T$ for *all* integers i.

Let $S \subset (\mathbb{Z}/m\mathbb{Z})^*$ be the set of residue classes $(a \bmod m)$ with the property that $\gcd(a, m) = 1$ and $a + m\mathbb{Z} \subset T$. We just proved that $(1 \bmod m)$, $(-1 \bmod m) \in S$, and one readily verifies that S is additively closed, as defined above (with m in the role of n). Hence, by what we proved above, we have $S = (\mathbb{Z}/m\mathbb{Z})^*$, and therefore every integer that is relatively prime to m belongs to T.

Now let $a \in \mathbb{Z}$, $\gcd(a, n) = 1$. For every prime number p dividing m, choose $a_p \in \mathbb{Z}$ such that $a_p \not\equiv 0 \bmod p$, $a_p \not\equiv a \bmod p$; this can be done since m is odd. Next, let $b \in \mathbb{Z}$ be such that $b \equiv a_p \bmod p$ for each prime number p dividing m. Then we have $\gcd(b, m) = \gcd(a-b, m) = 1$, so b, $a - b \in T$, and therefore $a = b + (a-b) \in T$. This proves Theorem 1.

Acknowledgements. The author thanks F. Alberto Grünbaum for suggesting the problem solved in this paper, and George Bergman, Everett Howe, and Carl Pomerance for helpful comments.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA 94720
U.S.A.

Received on 23.12.1992 (2361)