involve
a journal of mathematics

New algorithms for modular inversion and representation by the form $x^2 + 3xy + y^2$

Christina Doran, Shen Lu and Barry R. Smith

msp

2017 vol. 10, no. 4

INVOLVE 10:4 (2017)
dx.doi.org/10.2140/involve.2017.10.541

New algorithms for modular inversion and representation by the form $x^2 + 3xy + y^2$

Christina Doran, Shen Lu and Barry R. Smith

(Communicated by Filip Saidak)

We observe structure in the sequences of quotients and remainders of the Euclidean algorithm with two families of inputs. Analyzing the remainders, we obtain new algorithms for computing modular inverses and representing prime numbers by the binary quadratic form $x^2 + 3xy + y^2$. The Euclidean algorithm is commenced with inputs from one of the families, and the first remainder less than a predetermined size produces the modular inverse or representation.

1. The algorithms

Intuitively, the iterative nature of the Euclidean algorithm makes the sequences of quotients and remainders "sensitive to initial conditions". A small perturbation to the inputs can induce a chain reaction of increasingly large perturbations in the sequence of quotients and remainders, leading to considerable alterations to both the lengths of the sequences and their entries. Later entries are especially prone to change because of cumulative effects.

Our first result, Theorem 8, provides a surprising example of regularity under perturbation. When v is a solution of the congruence $v^2 + v - 1 \equiv 0 \pmod{u}$, we show that the Euclidean algorithm with u and $v - 1$ always takes one step fewer than the Euclidean algorithm with u and v. The sequences of quotients in both cases are almost identical, differing only in their middle one or two entries. (They are also symmetric outside of those middle entries.) We also obtain explicit formulas for the remainders of the Euclidean algorithm with u and $v - 1$ in terms of the remainders produced by u and v.

From these formulas we obtain a new algorithm for representing prime numbers by the indefinite quadratic form $x^2 + 3xy + y^2$. When such a representation exists,

MSC2010: 11A05.
Keywords: number theory, continued fraction, binary quadratic form, algorithm.
This work was supported by a grant from The Edward H. Arnold and Jeanne Donlevy Arnold Program for Experiential Education, which supports research experiences for undergraduates at Lebanon Valley College.

the algorithm produces one with $x > y > 0$. Lemma 3 at the end of this section shows this representation is unique.

Algorithm 1. *Let p be a prime number congruent to 1 or 4 modulo 5. To compute the unique representation $p = b^2 + 3bc + c^2$ with $b > c > 0$, first compute a solution v to the congruence $v^2 + v - 1 \equiv 0 \pmod{p}$, then perform the Euclidean algorithm with p and v. The first remainder less than $\sqrt{p/5}$ is c, and the remainder just preceding is either b or $b + c$.*

This algorithm is similar to earlier algorithms that use the Euclidean algorithm to produce representations by binary quadratic forms [Brillhart 1972; Cornacchia 1908; Hardy et al. 1990a; 1990b; Matthews 2002; Wilker 1980]. Of these, [Matthews 2002] is the only one to produce representations by forms with positive discriminant, namely, the forms $x^2 - wy^2$ with $w = 2, 3, 5, 6,$ or 7. The algorithm we present is a new contribution to this body of work.

We study a second family of inputs to the Euclidean algorithm, pairs $u > v$ for which $(v \pm 1)^2 \equiv 0 \pmod{u}$. This condition implies that there must exist a, b, and c with $u = ab^2$ and $v = abc \pm 1$. Theorems 9 and 10 give an explicit description of the quotients and remainders of the Euclidean algorithm with u and v in terms of the quotients and remainders of the Euclidean algorithm with b and c.

The relationship between the quotients of the Euclidean algorithm with b and c and with ab^2 and $abc \pm 1$ is essentially the "folding lemma" for continued fractions, first explicated independently in [Mendès France 1973; Shallit 1979]. This lemma has inspired a significant body of work concerning the quotients of continued fractions. These works give attention only to continued fractions — the remainders in the Euclidean algorithm are never explicitly considered. The description of the entire Euclidean algorithm with ab^2 and $abc \pm 1$ in Theorems 9 and 10 is new. They are unified by Theorem 11, which arithmetically characterizes the quotient pattern that will appear in the Euclidean algorithm with u and v when $(v \pm 1)^2 \equiv 0 \pmod{u}$.

Analysis of the remainders leads to another new algorithm, this time for modular inversion.

Algorithm 2. *If m and n are relatively prime positive integers, then the multiplicative inverse of m modulo n is the first remainder less than n when the Euclidean algorithm is performed with n^2 and $mn + 1$.*

A similar algorithm was obtained by Seysen [2005]. In his algorithm, an integer f is arbitrarily chosen with $f > 2n$, and the Euclidean algorithm is run with fn and $fm + 1$. The algorithm is stopped at the first remainder r less than $f + n$, and the modular inverse of m modulo n is then $r - f$ (which can be negative). If f were allowed to equal n, then this would be similar indeed to the algorithm above. However, Seysen's algorithm does not work generally in this case. For instance, with $n = 12$ and $m = 5$, Seysen's algorithm with $f = 12$ would say to run the

Euclidean algorithm with 144 and 61, stopping at the first remainder less than 24. This remainder is 22, and Seysen's algorithm would output 10, which is not an inverse for 5 modulo 12. Our algorithm above instead produces the inverse 5.

The inputs to Algorithm 2 are less than half the size of the inputs to Seysen's. But Seysen's algorithm has the flexibility arising from choosing the factor f. It would be interesting to see if both algorithms can fit in a common framework.

Our results are a new contribution to the literature on algorithmic number theory, but we believe the modular inversion algorithm also has pedagogical value. Students are less prone to mistakes working by hand with the new algorithm rather than the extended Euclidean algorithm or Blankinship's matrix algorithm [1963]. The new algorithm might seem nonintuitive, but our proof is elementary and is an amalgam of topics encountered by a student learning formal reasoning: the Euclidean algorithm, congruences, and mathematical induction.

We conclude this section with the result guaranteeing the uniqueness of the representation produced by Algorithm 1.

Lemma 3. *If p is a prime number congruent to* 1 *or* 4 *modulo* 5, *then there is a unique pair of positive integers $b > c$ satisfying*

$$p = b^2 + 3bc + c^2.$$

Proof. We work in the field $\mathbb{Q}(\sqrt{5})$. The algebraic integers in this field are

$$\mathcal{O} = \left\{ \tfrac{1}{2}m + \tfrac{1}{2}n\sqrt{5} : m, n, \in \mathbb{Z}, m \equiv n \mod 2 \right\}.$$

Denote by τ the nontrivial automorphism of $\mathbb{Q}(\sqrt{5})$ and by N the norm map $N\gamma = \gamma\gamma^\tau$. The unit $\varepsilon = \frac{3}{2} + \frac{1}{2}\sqrt{5}$ generates the group of units of norm 1 in $\mathbb{Z}[\sqrt{5}]$. The map

$$(b, c) \mapsto \left(b + \tfrac{3}{2}c\right) + \left(\tfrac{1}{2}c\right)\sqrt{5}$$

gives a bijection between all pairs of integers (b, c) with $b^2 + 3bc + c^2 = p$ and all elements of $\mathcal{O}$ of norm p. The condition $b > c > 0$ for a pair with $b^2 + 3bc + c^2 = p$ is equivalent to the corresponding element $\frac{1}{2}x + \frac{1}{2}y\sqrt{5}$ of $\mathcal{O}$ satisfying $x > 5y > 0$.

By quadratic reciprocity, p splits in $\mathbb{Q}(\sqrt{5})$. The ring $\mathcal{O}$ is a principal ideal domain, so we may pick a generator γ of one of the prime ideals dividing p. Multiplying γ by $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ if necessary, we may assume γ has norm p.

There is therefore at least one algebraic integer with norm p of the form $\frac{1}{2}x + \frac{1}{2}y\sqrt{5}$. Among all such elements, let α be one for which x is positive and is as small as possible (i.e., α has minimal positive trace). Replacing α by α^τ if necessary, we may assume also that y is positive. The lemma will be proved by showing that α is the unique element $\frac{1}{2}x + \frac{1}{2}y\sqrt{5}$ in $\mathcal{O}$ with norm p and $x > 5y > 0$.

Define a_n, b_n as the integers for which

$$\alpha\varepsilon^n = \tfrac{1}{2}a_n + \tfrac{1}{2}b_n\sqrt{5}.$$

Then

$$(\alpha\varepsilon^{-1})^{\tau} = \tfrac{1}{4}(3a_0 - 5b_0) + \tfrac{1}{4}(a_0 - 3b_0)\sqrt{5}.$$

If we suppose $a_0 - 3b_0 < 0$, then $\frac{1}{4}(5b_0 - 3a_0) > -\frac{1}{3}a_0$. If $5b_0 - 3a_0$ were negative, then $(\alpha\varepsilon^{-1})^{\tau}$ would have norm p and smaller positive trace than α, a contradiction. Thus, again by our choice of α, we have $\frac{1}{2}(5b_0 - 3a_0) \geq a_0$; hence $a_0 \leq b_0$. But then

$$N\alpha = \tfrac{1}{4}(a_0^2 - 5b_0^2) \leq -b_0^2 < 0,$$

which contradicts the assumption that α has norm p.

It must be then that $a_0 - 3b_0 > 0$, and thus, $3a_0 - 5b_0 > 0$. Again using our assumption on α, we have $\frac{1}{2}(3a_0 - 5b_0) \geq a_0$. It follows that $a_0 \geq 5b_0 > 0$ (and, in fact, $a_0 > 5b_0$ since $p \neq 5$).

It remains to show that α is the unique algebraic integer $\frac{1}{2}x + \frac{1}{2}y\sqrt{5}$ with norm p satisfying $x > 5y > 0$. Suppose x and y are integers and set $\frac{1}{2}w + \frac{1}{2}z\sqrt{5} = \left(\frac{1}{2}x + \frac{1}{2}y\sqrt{5}\right)\varepsilon$. It is readily checked that if $x > 0$ and $y > 0$, then $w > 0$ and $z > 0$ and $w < 5z$. It follows that all for all $n \geq 0$, we have $a_n > 0$ and $b_n > 0$, but $a_n > 5b_n$ only when $n = 0$. Recall that $\alpha\varepsilon^{-1} = \frac{1}{2}a_{-1} + \frac{1}{2}b_{-1}\sqrt{5}$. From the above two paragraphs, we have $a_{-1} > 0$ and $b_{-1} < 0$. If we set $\frac{1}{2}w' + \frac{1}{2}z'\sqrt{5} = \left(\frac{1}{2}x + \frac{1}{2}y\sqrt{5}\right)\varepsilon^{-1}$ and if $x > 0$ and $y < 0$, then $w' > 0$ and $y' < 0$. Thus, $a_n > 0$ and $b_n < 0$ for all $n \leq -1$.

The numbers in $\mathcal{O}$ of norm p are exactly $\pm\frac{1}{2}a_n \pm \frac{1}{2}b_n\sqrt{5}$ for n in $\mathbb{Z}$. It follows that the only possible element $\frac{1}{2}x + \frac{1}{2}y\sqrt{5}$ with norm p and $x > 5y > 0$ other than α is $\frac{1}{2}a_{-1} - \frac{1}{2}b_{-1}\sqrt{5} = \frac{1}{4}(3a_0 - 5b_0) + \frac{1}{4}(a_0 - 3b_0)\sqrt{5}$. But $3a_0 - 5b_0 > 5(a_0 - 3b_0)$ implies that $a_0 < 5b_0$, which we know is not true. The uniqueness is proved. □

2. Euclidean algorithm background

For positive integers $u > v$, the sequence of equations of the Euclidean algorithm when commenced by dividing v into u has the form

$$\begin{aligned} u &= q_1 v + r_1, \\ v &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{s-3} &= q_{s-1} r_{s-2} + r_{s-1}, \\ r_{s-2} &= q_s r_{s-1} + r_s, \end{aligned} \tag{1}$$

with $r_{s-1} = \gcd(u, v)$ and $r_s = 0$. We define

$$r_{-1} = u \quad \text{and} \quad r_0 = v.$$

Because $r_{s-1} < r_{s-2}$, it follows that $q_s \geq 2$.

Our study of the Euclidean algorithm is streamlined by allowing it to unfold in two different ways. These parallel the two continued fraction expansions of a rational number. The expansion of u/v with final quotient ≥ 2 is the sequence of quotients of the Euclidean algorithm with u and v. We will modify the Euclidean algorithm to make it produce the other expansion. If the Euclidean algorithm with u and v is written as (1), we replace the final equation by the two equations

$$r_{s-2} = (q_{s-1} - 1)r_{s-1} + r_{s-1}, \quad r_{s-1} = 1 \cdot r_{s-1} + 0. \tag{2}$$

This modification changes the length parities of the sequences of quotients and remainders.

Definition. If u and v are positive integers and $\delta = 0$ or 1, we denote by $\mathrm{EA}(u, v, \delta)$ the sequence of equations of the Euclidean algorithm when commenced with u and v. When $\delta = 0$, we use whichever of the standard or modified Euclidean algorithms takes an even number of steps, and when $\delta = 1$, whichever takes an odd number. When considering only the standard algorithm, we write simply $\mathrm{EA}(u, v)$. We denote the i-th equation by $\mathrm{EA}^i(u, v, \delta)$ or $\mathrm{EA}^i(u, v)$ and call the associated sequences (q_i) and (r_i) the *sequence of quotients* and *sequence of remainders*.

Reasoning about the Euclidean algorithm is facilitated by continuants. Properties of continuants can be found in Section 6.7 of the book by Graham, Knuth, and Patashnik [Graham et al. 1989].

Definition. Associated with a sequence $(q_1, \ldots, q_s)$ of integers, we define a doubly indexed sequence of *continuants*

$$\mathfrak{q}_{i,j} = q_i \mathfrak{q}_{i+1,j} + \mathfrak{q}_{i+2,j} \qquad \text{and} \qquad \mathfrak{q}_{i+1,i} = 1, \quad \mathfrak{q}_{i+2,i} = 0 \tag{3}$$

for $1 \leq i \leq j + 2 \leq s + 2$. When a more explicit description of the $\mathfrak{q}_i$ is required, we will use alternate notation (for $i \leq j$):

$$[q_i, \ldots, q_j] := \mathfrak{q}_{i,j}.$$

The properties of continuants that we will need are the recursion (3) and the surprising symmetry

$$[q_i, \ldots, q_j] = [q_j, \ldots, q_i],$$

which can be proved by induction. An illuminating combinatorial proof is in [Benjamin et al. 2000]. From the symmetry of continuants and recurrence (3) we obtain the alternate recurrence

$$\mathfrak{q}_{i,j} = q_j \mathfrak{q}_{i,j-1} + \mathfrak{q}_{i,j-2}. \tag{4}$$

Lemma 4. *Let u and v be relatively prime integers. If $(q_i)_{i=1}^{s}$ and $(r_i)_{i=-1}^{s}$ are the sequences of quotients and remainders of $\mathrm{EA}(u, v, \delta)$ and $\mathfrak{q}_{i,j}$ are the continuants corresponding to the sequence of quotients, then*

$$r_i = \mathfrak{q}_{i+2,s}$$

for $i = -1, \ldots, s$. In particular, $u = \mathfrak{q}_{1,s}$ and $v = \mathfrak{q}_{2,s}$.

Proof. Because u and v are relatively prime, we have $r_{s-1} = 1 = \mathfrak{q}_{s+1,s}$ and $r_s = 0 = \mathfrak{q}_{s+2,s}$. The formula $r_i = \mathfrak{q}_{i+2,s}$ follows from the observation that the recurrence (3) with $j = s$ is the same recurrence satisfied by the remainders. □

The continuants $\mathfrak{q}_{1,i}$ have a prominent role in studying the Euclidean algorithm. They are the numerators of the convergents of the simple continued fraction expansion of u/v, and they are the absolute values of coefficients commonly computed as part of the extended Euclidean algorithm. We therefore make the following definition.

Definition. Let $q_1, q_2, \ldots, q_s$ be the sequence of quotients of $\mathrm{EA}(u, v, \delta)$ with associated continuants $\mathfrak{q}_{i,j}$. We define the *Bézout coefficients* of u and v by

$$\beta_i = \mathfrak{q}_{1,i}$$

for $-1 \le i \le s$.

The following lemmas reveal a close connection between the sequence of remainders of $\mathrm{EA}(u, v, \delta)$ and the corresponding Bézout coefficients. Each makes a fine exercise in mathematical induction.

Lemma 5. *If $(q_i)_{i=1}^s$ and $(r_i)_{i=-1}^s$ are the sequences of quotients and remainders of* $\mathrm{EA}(u, v, \delta)$ *and $(\beta_i)_{i=-1}^s$ are the Bézout coefficients, then*

$$v\beta_i \equiv (-1)^i r_i \pmod{u} \quad \text{for } -1 \le i \le s.$$

Proof. The cases $i = -1$ and $i = 0$ simply say that $0 \equiv -u \pmod{u}$ and $v \equiv v \pmod{u}$. Further, if the congruence holds for $i-1$ and i with $0 \le i \le s-1$, then

$$\begin{aligned} v\beta_{i+1} &= vq_{i+1}\beta_i + v\beta_{i-1} \\ &\equiv (-1)^i q_{i+1} r_i + (-1)^{i-1} r_{i-1} \pmod{u} \\ &= (-1)^{i+1} r_{i+1}. \end{aligned}$$

The lemma follows by induction. □

Lemma 6. *If $(q_i)_{i=1}^s$ and $(r_i)_{i=-1}^s$ are the sequences of quotients and remainders of* $\mathrm{EA}(u, v, \delta)$ *and $(\beta_i)_{i=-1}^s$ are the Bézout coefficients, then $u = \beta_i r_{i-1} + \beta_{i-1} r_i$ for $0 \le i \le s$.*

Proof. For $i = 0$, the equation is just $u = u$. Assume that $u = \beta_i r_{i-1} + \beta_{i-1} r_i$ for some i with $0 \le i \le s-1$. Then using (4),

$$u = \beta_i(q_{i+1} r_i + r_{i+1}) + (\beta_{i+1} - q_{i+1}\beta_i) r_i = \beta_{i+1} r_i + \beta_i r_{i+1}.$$

The lemma follows by induction. □

We now discuss background for studying structure in the Euclidean algorithm quotients. Fix a positive integer k. In recent work [Smith 2015], it was proved that if v with $0 < v < u$ satisfies the congruence

$$v^2 + kv \pm 1 \equiv 0 \pmod{u},$$

then the sequence of quotients of $\mathrm{EA}(u, v, \delta)$ (with $\delta = 0$ if the plus sign is used in the above congruence and $\delta = 1$ otherwise) fits one of a finite list of "end-symmetric" patterns. The list of patterns depends only on k. We will use this result only when $k = 1$, 2, or 3.

Lemma 7. *The sequence of quotients of* $\mathrm{EA}(u, v, 1)$ *when* $v^2 + v - 1 \equiv 0 \pmod{u}$ *has the form*

$$q_1,\ \ldots,\ q_{s-1},\ q_s + (-1)^{s+1},\ 1,\ q_s,\ q_{s-1},\ \ldots,\ q_1$$

for some positive integers $q_1, \ldots, q_s$.

When $v^2 + 3v + 1 \equiv 0 \pmod{u}$, *then* $\mathrm{EA}(u, v, 0)$ *has quotient sequence of the form*

$$q_1,\ \ldots,\ q_{s-1},\ q_s + (-1)^{s+1} \cdot 3,\ q_s,\ q_{s-1},\ \ldots,\ q_1$$

for some positive integers $q_1, \ldots, q_s$.

When $v^2 + (-1)^{\delta} 2v + 1 \equiv 0 \pmod{u}$, *that is, when*

$$(v + (-1)^{\delta})^2 \equiv 0 \pmod{u}, \tag{5}$$

then $\mathrm{EA}(u, v, 0)$ *has quotient sequence fitting one of the patterns*

$$\begin{gathered} q_1,\ \ldots,\ q_{s-1},\ q_s - (-1)^{s+\delta},\ q_s + (-1)^{s+\delta},\ q_{s-1},\ \ldots,\ q_1, \\ q_1,\ \ldots,\ q_{s-1},\ q_s + 1,\ x,\ 1,\ q_s,\ q_{s-1},\ \ldots,\ q_1, \\ q_1,\ \ldots,\ q_{s-1},\ q_s - 1,\ 1,\ x,\ q_s,\ q_{s-1},\ \ldots,\ q_1 \end{gathered} \tag{6}$$

for some positive integers $q_1, \ldots, q_s$ *and* x.

The patterns (6) are well known, being related to paper-folding sequences and folded continued fractions [Shallit 1979; van der Poorten 2002]. What seems to be new is their appearance in the quotients of the Euclidean algorithm with u and v when v satisfies (5). Theorem 11 gives an arithmetical criteria for deciding which of the patterns (6) describes the simple continued fraction expansion of u/v.

3. Explicating the Euclidean algorithm

Suppose u and v are positive integers with $u > v$ and $v^2 + v - 1 \equiv 0 \pmod{u}$. Then $v - 1$ satisfies the congruence $v^2 + 3v + 1 \equiv 0 \pmod{u}$. According to Lemma 7, $\mathrm{EA}(u, v, 1)$ has sequence of quotients of the form $q_1, \ldots, q_s + \delta_1, 1, q_s + \delta_0, \ldots, q_1$, while $\mathrm{EA}(u, v - 1, 0)$ has sequence of quotients of the form $\tilde{q}_1, \ldots, \tilde{q}_s + \delta_1 \cdot 3$, $\tilde{q}_s + \delta_0 \cdot 3, \ldots, \tilde{q}_1$. In both cases, $\delta_1 = 1$ if s is odd and 0 if s is even, while $\delta_0 = 1$ if s is even and 0 if s is odd. There is no a priori reason for the sequence of q_i to equal the sequence of $\tilde{q}_i$. Nevertheless, that is the conclusion of the following theorem, which also gives explicit formulas for the remainders of $\mathrm{EA}(u, v - 1, 0)$ in terms of the remainders of $\mathrm{EA}(u, v, 1)$.

Theorem 8. *Let u and v be positive integers $u > v$, with $v^2 + v - 1 \equiv 0 \pmod{u}$. Write the sequence of quotients of* $\mathrm{EA}(u, v, 1)$ *as*

$$q_1,\ \ldots,\ q_s + \delta_1,\ 1,\ q_s + \delta_0,\ \ldots,\ q_1.$$

Let $(r_i)_{i=-1}^{2s+1}$ be the sequence of remainders, and for $i = -1, \ldots, s-1$, set

$$t_i = r_i + (-1)^{i+1} r_{2s-i}.$$

Then $\mathrm{EA}(u, v-1, 0)$ *is the sequence of $2s$ equations*

$$\begin{aligned}
t_{i-2} &= q_i \cdot t_{i-1} + t_i && \text{for } 1 \le i \le s-1,\\
t_{s-2} &= (q_s + \delta_1 \cdot 3) \cdot t_{s-1} + r_{s+1},\\
t_{s-1} &= (q_s + \delta_0 \cdot 3) \cdot r_{s+1} + r_{s+2},\\
r_{i-1} &= q_{2s+1-i} \cdot r_i + r_{i+1} && \text{for } s+2 \le i \le 2s.
\end{aligned}$$

Proof. A quick check verifies that $t_{-1} = u$ and $t_0 = v - 1$, which begin the remainder sequence of $\mathrm{EA}(u, v-1, 0)$. Because the sequence $(r_i)_{i=1}^{2s+1}$ is decreasing, it is clear that the purported quotients and remainders are all positive. We check that the purported remainders form a strictly decreasing sequence (except that the final two may be equal when $\mathrm{EA}(u, v-1, 0)$ is computed using the modification (2) of the Euclidean algorithm.) This is apparent for $r_{s+1}, \ldots, r_{2s+1}$. Also, $t_{s-1} \ge r_{s-1} - r_{s+1} = r_s \ge r_{s+1}$. (The equality is because the middle quotient of $\mathrm{EA}(u, v, 1)$ is 1. The final equality is strict unless $u = 5$ and $v = 2$.)

We must show $t_i > t_{i+1}$ for $1 \le i \le s-2$. From the division algorithm, we have $r_i \ge r_{i+1} + r_{i+2}$ for $-1 \le i \le 2s-1$. Thus, for $-1 \le i \le s-3$, we have

$$r_i - r_{i+1} \ge r_{i+2} \ge r_{i+3} + r_{i+4} > r_{2s-i} + r_{2s-i-1}.$$

It follows that $t_i > t_{i+1}$ for $1 \le i \le s-3$. The above chain of inequalities also holds with the final inequality replaced by an equality when $i = s-2$. The second inequality is strict when $i = s-2$ unless $q_s + \delta_0 = 1$, which only happens if s is odd. But in that case, $t_{s-2} = r_{s-2} + r_{s+2} > r_{s-1} - r_{s+1} = t_{s-1}$ holds anyway.

To ensure the equations in the theorem are the steps of $\mathrm{EA}(u, v-1, 0)$, it remains to check the algebraic validity of each step. The theorem will then follow from the uniqueness of the quotients and remainders.

The equation $t_{i-2} = q_i \cdot t_{i-1} + t_i$ is equivalent to

$$(-1)^{i+1}(r_{i-2} - q_i r_{i-1} - r_i) = r_{2s-i} - q_i r_{2s+1-i} - r_{2s+2-i}.$$

The expression on the left is 0. Also, examining the pattern of the sequence of quotients of $\mathrm{EA}(u, v, 1)$, we see that $q_{2s+2-i} = q_i$ for $i = 1, \ldots, s-1$. Thus, the

$(2s-i+1)$-th step of EA$(u, v, 1)$ is

$$r_{2s-i} = q_i r_{2s+1-i} + r_{2s+2-i}, \tag{7}$$

and the right side is also 0. Substituting $2s+1-i$ for i in (7), we find as well that $r_{i-1} = q_{2s+1-i} r_i + r_{i+1}$ for $s+2 \le i \le 2s$, which verifies steps $i = s+2$ through $i = 2s$ in the theorem.

We now check the middle pair of equations. We know that the s-th through $(s+2)$-th equations of EA$(u, v, 1)$ are

$$\begin{aligned} r_{s-2} &= (q_s + \delta_1) r_{s-1} + r_s, \\ r_{s-1} &= \qquad\quad r_s \quad + r_{s+1}, \\ r_s &= (q_s + \delta_0) r_{s+1} + r_{s+2}. \end{aligned} \tag{8}$$

Assume first that s is odd so that $\delta_1 = 1$ and $\delta_0 = 0$. The equation

$$t_{s-2} = (q_s + \delta_1 \cdot 3) t_{s-1} + r_{s+1}$$

is equivalent to

$$r_{s-2} = (q_s + 3)(r_{s-1} - r_{s+1}) + r_{s+1} - r_{s+2}.$$

Substituting in turn $r_{s+2} = r_s - q_s r_{s+1}$ and $r_{s+1} = r_{s-1} - r_s$ from (8), this is equivalent to

$$\begin{aligned} r_{s-2} &= (q_s + 3)(r_{s-1} - r_{s+1}) + r_{s+1} - r_s + q_s r_{s+1} \\ &= (q_s + 3) r_s + r_{s-1} - 2r_s + q_s r_{s-1} - q_s r_s \\ &= (q_s + 1) r_{s-1} + r_s, \end{aligned}$$

which is the first of equations (8).

If, instead, s is even, so $\delta_1 = 0$ and $\delta_0 = 1$, then $t_{s-2} = (q_s + \delta_1 \cdot 3) t_{s-1} + r_{s+1}$ is equivalent to

$$r_{s-2} = q_s (r_{s-1} + r_{s+1}) + r_{s+1} + r_{s+2}.$$

Substituting in turn $r_{s+2} = r_s - q_s r_{s+1} - r_{s+1}$ and $r_{s+1} = r_{s-1} - r_s$, this is equivalent to

$$\begin{aligned} r_{s-2} &= q_s (r_{s-1} + r_{s+1}) + r_s - q_s r_{s+1} \\ &= q_s (2r_{s-1} - r_s) + r_s - q_s r_{s-1} + q_s r_s \\ &= q_s r_{s-1} + r_s, \end{aligned}$$

which is the first of equations (8).

The verification that $t_{s-1} = (q_s + \delta_0 \cdot 3) \cdot r_{s+1} + r_{s+2}$ is entirely similar, using the latter two equations of (8). □

Proof of Algorithm 1. Let the quotients and remainders of EA$(u, v, 1)$ be written as in Theorem 8. Suppose first that s is odd. Applying Lemma 6 with $i = s$ to

EA$(u, v, 1)$, we have $u = [q_1, \ldots, q_{s-1}, q_s + 1]r_{s-1} + [q_1, \ldots, q_{s-1}]r_s$. By the symmetry of continuants and recurrence (4), it follows that

$$\begin{aligned} u &= [q_s + 1, q_{s-1}, \ldots, q_1]r_{s-1} + [q_{s-1}, \ldots, q_1]r_s \\ &= [q_{s-1}, \ldots, q_1](r_{s-1} + r_s) + [q_s, \ldots, q_1]r_{s-1}. \end{aligned}$$

Now use the "end-symmetric" form of the quotient sequence of EA$(u, v, 1)$ and Lemma 4 to obtain

$$u = r_{s+1}(r_{s-1} + r_s) + r_s r_{s-1}.$$

Substituting out r_{s-1} using the middle of equations (8) gives

$$u = r_s^2 + 3r_s r_{s+1} + r_{s+1}^2.$$

Suppose now that s is even. Applying Lemma 6 with $i = s$ to EA$(u, v, 1)$ in this case gives $u = [q_1, \ldots, q_s]r_{s-1} + [q_1, \ldots, q_{s-1}]r_s$. Again using the recurrence (4), it follows that

$$u = [q_s + 1, q_{s-1}, \ldots, q_1]r_{s-1} + [q_{s-1}, \ldots, q_1](r_s - r_{s-1}),$$

and Lemma 4 shows

$$u = r_s r_{s-1} + r_{s+1}(r_s - r_{s-1}).$$

Substituting with (8) once more gives

$$u = (r_s - r_{s+1})^2 + 3(r_s - r_{s+1})r_{s+1} + r_{s+1}^2.$$

Thus, in either case, $r_{s+1} = c$ in the unique representation $p = b^2 + 3bc + c^2$ with $b > c > 0$. If s is odd, then $r_s = b$, and if s is even, then $r_s = b + c$. The inequalities $5b^2 > b^2 + 3bc + c^2 > 5c^2$ show that

$$b + c > b > \sqrt{\frac{p}{5}} > c.$$

Therefore regardless of whether s is odd or even, c is the first remainder smaller than $\sqrt{p/5}$. □

Fix anew positive integers b and c with $\gcd(b, c) = 1$. We next give an explicit description of the quotients and remainders of EA$(b^2, bc \pm 1)$ in terms of the quotients, remainders, and Bézout coefficients of EA(b, c). The algorithm for computing inverses in modular arithmetic falls out of this description.

Theorem 9. *Let $b > c > 1$ be integers with $\gcd(b, c) = 1$. Let $(q_i)_{i=1}^{s}$ and $(r_i)_{i=-1}^{s}$ be the sequences of quotients and remainders of the standard (i.e., unmodified) Euclidean algorithm with b and c, let $(\beta_i)_{i=-1}^{s}$ be the corresponding Bézout coefficients, and set $t_i = r_i b \pm (-1)^i \beta_i$ for $-1 \le i \le s - 1$. Then* EA$(b^2, bc \pm 1, 0)$ *is the*

sequence of $2s$ *equations*

$$\begin{aligned}
t_{i-2} &= q_i \cdot t_{i-1} + t_i && \text{for } 1 \le i \le s-1,\\
t_{s-2} &= (q_s \pm (-1)^s) \cdot t_{s-1} + \beta_{s-1},\\
t_{s-1} &= (q_s \pm (-1)^{s-1}) \cdot \beta_{s-1} + \beta_{s-2},\\
\beta_{2s+1-i} &= q_{2s+1-i} \cdot \beta_{2s-i} + \beta_{2s-1-i} && \text{for } s+2 \le i \le 2s.
\end{aligned}$$

Proof. The proof can be conducted in an analogous manner to the proof of Theorem 8. One readily checks that the first two remainders are $t_{-1} = b^2$ and $t_0 = bc \pm 1$. The observation $q_s \ge 2$ was made in the first paragraph of Section 2, so the purported quotients are all positive. So are the remainders since $b \ge \beta_i$ for $-1 \le i \le s-1$.

For $s+2 \le i \le 2s$, the equation $\beta_{2s+1-i} = q_{2s+1-i} \cdot \beta_{2s-i} + \beta_{2s-1-i}$ follows from (4). For $1 \le i \le s-1$, the equality $t_{i-2} = q_i t_{i-1} + t_i$ can be deduced from the equation $\mathrm{EA}^i(b, c)$ and (4). To verify the middle two equations, we first note that because b and c are relatively prime, we have $r_{s-1} = 1$, $t_{s-1} = b \pm (-1)^{s-1}\beta_{s-1}$, and $q_s = r_{s-2}$. The equations can then be verified using Lemma 6 with $u = b$, $v = c$, and $i = s-1$:

$$\begin{aligned}
(q_s \pm (-1)^s)t_{s-1} + \beta_{s-1} &= (r_{s-2} \pm (-1)^s)b \pm (-1)^{s-1} r_{s-2}\beta_{s-1}\\
&= r_{s-2}\, b \pm (-1)^{s-2}\beta_{s-2}\\
&= t_{s-2}
\end{aligned}$$

and

$$\begin{aligned}
(q_s \pm (-1)^{s-1})\beta_{s-1} + \beta_{s-2} &= r_{s-2}\beta_{s-1} \pm (-1)^{s-1}\beta_{s-1} + \beta_{s-2}\\
&= b \pm (-1)^{s-1}\beta_{s-1}\\
&= t_{s-1}.
\end{aligned}$$

Finally, the remainders form a decreasing sequence. For $-1 < i < s-1$, the inequality $(r_i - r_{i+1})b > \beta_i + \beta_{i+1}$ follows from Lemma 6 and implies $t_i > t_{i+1}$. The inequality $\beta_{s-1} < t_{s-1}$ follows from the equation $t_{s-1} = (q_s \pm (-1)^{s-1})\beta_{s-1} + \beta_{s-2}$ verified in the last paragraph. And $\beta_{i-1} < \beta_i$ for $0 \le i \le s$ follows from the recurrence (4). □

Proof of Algorithm 2. When $m = 1$, the algorithm is easily validated. If $m > n$, then the third step of $\mathrm{EA}(n^2, mn+1)$ will be division of $rn+1$ into n^2, where r is the remainder when m is divided by n. Thus, it suffices to assume $n > m > 1$, so also $s > 1$.

Theorem 9 implies the first remainder less than n in $\mathrm{EA}(n^2, mn+1)$ is β_{s-1} when s is odd and t_{s-1} when s is even. We apply Lemma 5 to $\mathrm{EA}(n, m)$ to find $m\beta_{s-1} \equiv (-1)^{s-1} \pmod{n}$. Thus when s is odd, the product of m and the first

remainder less than n is

$$m\beta_{s-1} \equiv 1 \pmod{n}.$$

When s is even, the product is

$$mt_{s-1} = mn - m\beta_{s-1} \equiv 1 \pmod{n}. \qquad \square$$

We now give a complete description of $\mathrm{EA}(ab^2, abc \pm 1)$ for positive integers $a \geq 2$, b, and c and $\gcd(b, c) = 1$.

Theorem 10. *Let a, b, c, and k be integers with $b > c > 1$, $\gcd(b, c) = 1$, and $a \geq 2$. Let $(q_i)_{i=1}^{s}$ and $(r_i)_{i=-1}^{s}$ be the sequences of quotients and remainders in $\mathrm{EA}(b, c)$, let $(\beta_i)_{i=-1}^{s}$ be the corresponding Bézout coefficients, and set $t_i = abr_i + (-1)^{i+k}\beta_i$ for $-1 \leq i \leq s-1$. If $(-1)^{s+k} = -1$, then $\mathrm{EA}(ab^2, abc + (-1)^k, 0)$ is the sequence of $2s+2$ equations*

$$\begin{aligned}
t_{i-2} &= q_i \cdot t_{i-1} + t_i && \text{for } 1 \leq i \leq s-1,\\
t_{s-2} &= (q_s - 1) \cdot t_{s-1} + (t_{s-1} - b),\\
t_{s-1} &= 1 \cdot (t_{s-1} - b) + b,\\
t_{s-1} - b &= (a-1) \cdot b + \beta_{s-1},\\
b &= q_s \cdot \beta_{s-1} + \beta_{s-2},\\
\beta_{2s+3-i} &= q_{2s+3-i} \cdot \beta_{2s+2-i} + \beta_{2s+1-i} && \text{for } s+4 \leq i \leq 2s+2.
\end{aligned}$$

When $(-1)^{s+k} = 1$, steps s through $s+3$ change to

$$\begin{aligned}
t_{s-2} &= q_s \cdot t_{s-1} + b,\\
t_{s-1} &= (a-1) \cdot b + (b - \beta_{s-1}),\\
b &= 1 \cdot (b - \beta_{s-1}) + \beta_{s-1},\\
b - \beta_{s-1} &= (q_s - 1) \cdot \beta_{s-1} + \beta_{s-2}.
\end{aligned}$$

Proof. It follows as in the proof of Theorem 9 that the purported quotients and remainders are positive (excluding the final remainder). The equations $\beta_{2s+3-i} = q_{2s+3-i} \cdot \beta_{2s+2-i} + \beta_{2s+1-i}$ and $t_{i-2} = q_i t_{i-1} + t_i$ can be deduced as in the proof of Theorem 9. The equations $t_{s-1} = 1 \cdot (t_{s-1} - b) + b$ and $b = 1 \cdot (b - \beta_{s-1}) + \beta_{s-1}$ are clearly true. Lemma 4 shows that $\beta_s = b$. Thus, the equations $b = q_s \cdot \beta_{s-1} + \beta_{s-2}$ and $b - \beta_{s-1} = (q_s - 1)\beta_{s-1} + \beta_{s-2}$ are consequences of (4).

Since $\gcd(b, c) = 1$, we have $r_{s-1} = 1$, $t_{s-1} = ab - (-1)^{s+k}\beta_{s-1}$, and $q_s = r_{s-2}$. From this, we obtain the equations $t_{s-1} - b = (a-1)b + \beta_{s-1}$ when $(-1)^{s+k} = -1$ and $t_{s-1} = (a-1)b + (b - \beta_{s-1})$ when $(-1)^{s+k} = 1$.

When $(-1)^{s+k} = -1$, the s-th equation is valid since

$$\begin{aligned}(q_s - 1)t_{s-1} + (t_{s-1} - b) &= q_s(ab + \beta_{s-1}) - \beta_s \\ &= abr_{s-2} + (\beta_s - \beta_{s-2}) - \beta_s, \\ &= t_{s-2}.\end{aligned}$$

Similarly, when $(-1)^{s+k} = 1$,

$$\begin{aligned}q_s t_{s-1} + b &= q_s(ab - \beta_{s-1}) + b \\ &= abr_{s-2} - (\beta_s - \beta_{s-2}) + \beta_s \\ &= t_{s-2}.\end{aligned}$$

When $(-1)^{s+k} = -1$, the inequality $t_{s-1} - b < t_{s-1}$ is clear and the inequality $b < t_{s-1} - b$ follows from the assumption that $a \geq 2$. When $(-1)^{s+k} = 1$, the inequality $b < t_{s-1}$ follows from the assumption that $a \geq 2$ and from $b = \beta_s > \beta_{s-1}$. The inequality $b - \beta_{s-1} < b$ is clear, and the inequality $\beta_{s-1} < b - \beta_{s-1}$ follows from $b = q_s\beta_{s-1} + \beta_{s-2}$ and $q_s \geq 2$. That $t_i < t_{i-1}$ and $\beta_i > \beta_{i-1}$ for $1 \leq i \leq s-1$ follows as in the proof of Theorem 9. □

To conclude, we provide an arithmetical characterization of which quotient pattern will appear when performing the Euclidean algorithm with u and v with $(v \pm 1)^2 \equiv 0 \pmod{u}$.

Theorem 11. *Let u be a positive integer and write $u = ab^2$, where a is the square-free part of u. Assume v with $0 < v < u$ satisfies $(v + (-1)^\delta)^2 \equiv 0 \pmod{u}$. Then there is an integer c such that*

$$v = abc + (-1)^{\delta+1}.$$

Let $q_1, \ldots, q_s$ be the quotient sequence of the simple continued fraction expansion of b/c.

The continued fraction expansion of u/v with even length has quotient sequence fitting the first of the patterns (6) if and only if $\gcd(b, c) = a = 1$. Otherwise, it fits one of the other patterns with $x = \gcd(b, c)^2 \cdot a - 1$. The second pattern appears if $s + \delta$ is odd, and the third if $s + \delta$ is even.

Proof. By assumption, there exists some integer w such that $(v + (-1)^\delta)^2 = uw$. Consideration of prime factorizations shows that a is also the square-free part of w, say $w = ac^2$. Then $v = abc + (-1)^{\delta+1}$.

If $\gcd(b, c) = d$ and we set $\tilde{a} = ad^2$, $\tilde{b} = b/d$, and $\tilde{c} = c/d$, then

$$u = \tilde{a}\tilde{b}^2, \quad v = \tilde{a}\tilde{b}\tilde{c} + (-1)^{\delta+1}, \quad \text{and} \quad \gcd(\tilde{b}, \tilde{c}) = 1.$$

Theorem 11 now follows from Theorem 9 and Theorem 10. □

References

[Benjamin et al. 2000] A. T. Benjamin, F. E. Su, and J. J. Quinn, "Counting on continued fractions", *Math. Mag.* **73**:2 (2000), 98–104. MR

[Blankinship 1963] W. A. Blankinship, "Classroom notes: a new version of the Euclidean algorithm", *Amer. Math. Monthly* **70**:7 (1963), 742–745. MR Zbl

[Brillhart 1972] J. Brillhart, "Note on representing a prime as a sum of two squares", *Math. Comp.* **26** (1972), 1011–1013. MR Zbl

[Cornacchia 1908] G. Cornacchia, "Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$", *Giorn. Mat. Battaglini* **46** (1908), 33–90. JFM

[Graham et al. 1989] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics: a foundation for computer science*, Addison-Wesley, Reading, MA, 1989. MR Zbl

[Hardy et al. 1990a] K. Hardy, J. B. Muskat, and K. S. Williams, "A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v", *Math. Comp.* **55**:191 (1990), 327–343. MR Zbl

[Hardy et al. 1990b] K. Hardy, J. B. Muskat, and K. S. Williams, "Solving $n = au^2 + buv + cv^2$ using the Euclidean algorithm", *Utilitas Math.* **38** (1990), 225–236. MR Zbl

[Matthews 2002] K. Matthews, "Thue's theorem and the Diophantine equation $x^2 - Dy^2 = \pm N$", *Math. Comp.* **71**:239 (2002), 1281–1286. MR Zbl

[Mendès France 1973] M. Mendès France, "Sur les fractions continues limitées", *Acta Arith.* **23**:2 (1973), 207–215. MR Zbl

[van der Poorten 2002] A. J. van der Poorten, "Symmetry and folding of continued fractions", *J. Théor. Nombres Bordeaux* **14**:2 (2002), 603–611. MR Zbl

[Seysen 2005] M. Seysen, "Using an RSA accelerator for modular inversion", pp. 226–236 in *Cryptographic hardware and embedded systems – CHES 2005* (Edinburgh, 2005), edited by J. R. Rao and B. Sunar, Lecture Notes in Computer Science **3659**, Springer, Berlin, 2005.

[Shallit 1979] J. Shallit, "Simple continued fractions for some irrational numbers", *J. Number Theory* **11**:2 (1979), 209–217. MR Zbl

[Smith 2015] B. R. Smith, "End-symmetric continued fractions and quadratic congruences", *Acta Arith.* **167**:2 (2015), 173–187. MR Zbl

[Wilker 1980] P. Wilker, "An efficient algorithmic solution of the Diophantine equation $u^2+5v^2=m$", *Math. Comp.* **35**:152 (1980), 1347–1352. MR Zbl

Received: 2013-09-10 Revised: 2015-05-06 Accepted: 2016-07-11

christina.doran@chubb.com *Lebanon Valley College, 101 College Ave., Annville, PA 17003, United States*

shlu6807@colorado.edu *Lebanon Valley College, 101 College Ave., Annville, PA 17003, United States*

barsmith@lvc.edu *Lebanon Valley College, 101 College Ave., Annville, PA 17003, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2017 is US $175/year for the electronic version, and $235/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve
2017 vol. 10 no. 4