#A29 INTEGERS 24 (2024)

THE EUCLIDEAN ALGORITHM AS A SEQUENCE OF MODULAR INVERSE SWITCHING FORMULAS

Spiros Konstantogiannis
Ronin Institute, Montclair, New Jersey
spiros.konstantogiannis@ronininstitute.org

Received: 6/26/23, Revised: 12/9/23, Accepted: 2/16/24, Published: 3/15/24

Abstract

We show that every equation that is derived by the application of the Euclidean algorithm to two coprime positive integers can be written as a modular inverse switching formula, and this allows us to provide a backward recurrence relation for computing modular inverses. Using the recurrence relation, we then give an alternative proof of a theorem due to Rankin, which states that for two positive integers, the pair of Bézout coefficients that is provided by the Euclidean algorithm is, as a point in the plane, nearest to the origin. We also derive bounds on the two Bézout coefficients and we examine when the bounds can be sharpened.

1. Introduction

Modular inversion is a key operation in modular arithmetic, with many important practical and theoretical applications, as in public-key cryptography and in solvability of systems of linear congruences by the Chinese remainder theorem [5, 7]. The extended Euclidean algorithm, which is based on the Euclidean algorithm, is the standard method for computing modular inverses [5, 7]. In this work, we derive a modular inverse switching formula and we show that every equation provided by the application of the Euclidean algorithm to two coprime positive integers can take the form of the derived switching formula yielding a backward recurrence relation for computing modular inverses. Next, using the derived recurrence relation, we show that for two positive integers m and n, the pair of Bézout coefficients that is provided by the Euclidean algorithm is such that the coefficient of m is the least absolute inverse of $\frac{m}{\gcd(m,n)}$ modulo $\frac{n}{\gcd(m,n)}$, and likewise, the coefficient of n is the least absolute inverse of $\frac{n}{\gcd(m,n)}$ modulo $\frac{m}{\gcd(m,n)}$. This allows us to show that the pair of Bézout coefficients that is provided by the Euclidean algorithm is, as a point in the plane, nearest to the origin, which is a result already obtained by Rankin [6] using induction on the number of steps in the Euclidean algorithm. Finally, we

DOI: 10.5281/zenodo.10821707

derive bounds on the two Bézout coefficients that slightly improve those given by Rankin, and we examine when the bounds can be sharpened.

2. Modular Inverse Switching

In what follows, if an integer a is invertible modulo a positive integer n, then we denote by $a^{-1} \bmod n$ the inverse of a modulo n, which is unique modulo n.

Lemma 1. *Let m and n be coprime positive integers. If (x, y) is a pair of Bézout coefficients for (m, n), then $x = m^{-1} \bmod n$ and $y = n^{-1} \bmod m$.*

Proof. Let (x, y) be a pair of Bézout coefficients for (m, n). As a result,

$$xm + yn = 1. \tag{1}$$

By Equation (1), we have $xm \equiv 1 \pmod{n}$ and $yn \equiv 1 \pmod{m}$. As a result, $x = m^{-1} \bmod n$ and $y = n^{-1} \bmod m$. □

Remark 1. Substituting the expressions of x and y into Equation (1) and solving for $m^{-1} \bmod n$, we obtain

$$m^{-1} \bmod n = \frac{1 + n(-n^{-1} \bmod m)}{m}. \tag{2}$$

Equation (2) is known as Arazi's inversion formula and is used to compute the inverse of m modulo n from the inverse of n modulo m [2, 4].

Lemma 2. *Let m and n be positive integers, let t be an integer, and let both m and t be coprime to n. There exists an integer k such that $m = kn + t$ if and only if*

$$(t^{-1} \bmod n)m + (n^{-1} \bmod m)n = 1. \tag{3}$$

Proof. Let there exist an integer k such that $m = kn + t$. As a result, $m \equiv t \pmod{n}$. Also, both m and t are invertible modulo n, since both m and t are coprime to n. Thus, $m^{-1} \bmod n = t^{-1} \bmod n$. Besides, by Lemma 1, we have $(m^{-1} \bmod n)m+(n^{-1} \bmod m)n = 1$ and substituting the expression of $m^{-1} \bmod n$, we arrive at Equation (3).

Now, let Equation (3) hold. Since m and n are coprime and positive, it follows from Lemma 1 that $(m^{-1} \bmod n)m + (n^{-1} \bmod m)n = 1$. Subtracting Equation (3) from the last equation yields $(m^{-1} \bmod n - t^{-1} \bmod n)m = 0$, and since m is nonzero, we have $m^{-1} \bmod n = t^{-1} \bmod n$, whence $m \equiv t \pmod{n}$, and thus there exists an integer k such that $m = kn + t$. □

Remark 2. Solving Equation (3) for $t^{-1} \bmod n$, we express the inverse of t modulo n in terms of the inverse of n modulo m, while solving for $n^{-1} \bmod m$, we express the inverse of n modulo m in terms of the inverse of t modulo n, and taking into account that $m = kn + t$, this can be considered as modular inverse switching (or shifting). For this reason, we call Equation (3) a modular inverse switching formula.

3. The Euclidean Algorithm as a Sequence of Modular Inverse Switching Formulas

Let m and n be positive integers. We assume that m is not a multiple of n and n is not a multiple of m, either, so that the Euclidean algorithm provides a pair of Bézout coefficients for m and n. As a result, both integers m and n are greater than 1 and they are not equal. Hence, without loss of generality, we assume that $m > n > 1$. Since m and n are not both zero, it follows that $\gcd(m, n)$ exists in positive integers. Further, since $n \nmid m$, we have that n is not a common divisor of m and n. Also, since n is positive, it follows that n is the greatest divisor of itself. As a result, $\gcd(m, n) < n$, and combining with $m > n > 1$, we obtain $m > n > \gcd(m, n) \geq 1$, whence $\frac{m}{\gcd(m,n)} > \frac{n}{\gcd(m,n)} > 1$, and setting $r_0 = \frac{m}{\gcd(m,n)}$ and $r_1 = \frac{n}{\gcd(m,n)}$, we get $r_0 > r_1 > 1$, and r_0 and r_1 are coprime. Next, applying the Euclidean algorithm to r_0 and r_1 yields that there exists a positive integer n such that for every $i = 1, \ldots, n$, we have

$$r_{i-1} = q_i r_i + r_{i+1}, \tag{4}$$

where $r_2, \ldots, r_{n+1}$ are positive integers and $r_0 > r_1 > \ldots > r_{n+1} = 1$, and where $q_1, \ldots, q_n$ are also positive integers. We note that $r_{n+1} = \gcd(r_0, r_1)$. By Equation (4), we have $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i)$ for every $i = 1, \ldots, n$, and since $\gcd(r_0, r_1) = 1$, successive application of the previous equation yields that $\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i) = 1$ for every $i = 1, \ldots, n$. Hence, both r_{i-1} and r_{i+1} are coprime to r_i for every $i = 1, \ldots, n$. Thus, by Lemma 2, for every $i = 1, \ldots, n$, Equation (4) is equivalent to $(r_{i+1}^{-1} \bmod r_i)r_{i-1} + (r_i^{-1} \bmod r_{i-1})r_i = 1$, and setting $r_j^{-1} = r_j^{-1} \bmod r_{j-1}$ for every $j = 1, \ldots, n+1$, we arrive at

$$r_{i+1}^{-1} r_{i-1} + r_i^{-1} r_i = 1. \tag{5}$$

We have thus transformed the system of Equations (4) into the system of Equations (5), where for every $i = 1, \ldots, n$, the i-th equation of the former is equivalent to the i-th equation of the latter. Further, for $i = n$, Equations (4) and (5) read $r_{n-1} + (-q_n)r_n = 1$ and $r_{n+1}^{-1} r_{n-1} + r_n^{-1} r_n = 1$, respectively, and treating r_{n-1} and r_n as independent variables, we derive that

$$r_{n+1}^{-1} = 1. \tag{6}$$

We note that, since $r_{n+1} = 1$, the inverse r_{n+1}^{-1} of r_{n+1} modulo r_n is $1 + kr_n$, where k is an integer. However, as we showed comparing Equations (4) and (5) for $i = n$, the Euclidean algorithm provides the value 1 for r_{n+1}^{-1}.

Equation (5) can be written as

$$r_i^{-1} = \frac{1 - r_{i+1}^{-1} r_{i-1}}{r_i}, \tag{7}$$

for every $i = 1, \ldots, n$. In view of Equation (6), Equation (7) yields a unique inverse r_i^{-1} for every $i = 1, \ldots, n$. Since it gives the inverse of r_i modulo r_{i-1} in terms of the inverse of r_{i+1} modulo r_i, Equation (7) is a two-term backward recurrence relation for computing modular inverses. It is important to note that Equation (7) uses, as inputs, only the given integers r_0 and r_1, and the remainders $r_2, \ldots, r_n$ that are provided by the Euclidean algorithm; it does not use the quotients $q_1, \ldots, q_n$.

Variants of the extended Euclidean algorithm that use three-term backward recurrence relations are described by Glasby [1]. Equation (7) is a two-term recurrence relation. However, apart from a multiplication and an addition (subtraction), Equation (7) also involves a division, contrary to the relations described by Glasby, which involve only multiplications and additions (subtractions). On the other hand, the division in Equation (7) is exact for every $i = 1, \ldots, n$, and fast algorithms for exact division have long been available (see, for instance, [3]). Also, Equation (7) is suitable for computing modular inverses with the use of a hand calculator.

Example 1. We will compute the inverse of 779 modulo 2141. The integer 2141 is prime and does not divide 779; thus, 779 and 2141 are coprime. As a result, 779 is invertible modulo 2141. Applying the Euclidean algorithm to 2141 and 779 yields the following equations:

$$\begin{aligned} 2141 &= 2 \cdot 779 + 583, \\ 779 &= 583 + 196, \\ 583 &= 2 \cdot 196 + 191, \\ 196 &= 191 + 5, \\ 191 &= 38 \cdot 5 + 1. \end{aligned}$$

Hence, following our notation, we have $r_0 = 2141$, $r_1 = 779$, and the sequence of remainders $r_2 = 583$, $r_3 = 196$, $r_4 = 191$, $r_5 = 5$, and $r_6 = 1$. Next, taking into account that $r_6^{-1} = 1$, successive application of Equation (7) yields $r_5^{-1} = \frac{1-r_4}{r_5} = -38$, $r_4^{-1} = \frac{1-r_5^{-1}r_3}{r_4} = 39$, $r_3^{-1} = \frac{1-r_4^{-1}r_2}{r_3} = -116$, $r_2^{-1} = \frac{1-r_3^{-1}r_1}{r_2} = 155$, and $r_1^{-1} = \frac{1-r_2^{-1}r_0}{r_1} = -426$. Consequently, the inverse of 779 modulo 2141 is equal to -426; i.e., $779^{-1} \bmod 2141 = -426$.

If an integer a is invertible modulo a positive integer n, then the inverse of a modulo n is unique modulo n. This means that if x is an inverse of a modulo n, then the residue class of x modulo n contains exactly the inverses of a modulo n. As a result, every complete system of residues modulo n contains a unique inverse of a modulo n. We call the unique inverse of a modulo n that is contained in the complete system of least absolute residues modulo n, the least absolute inverse of a modulo n. We note that if n is even, then the complete system of least absolute residues modulo n is the set $\{-(\frac{n}{2}-1),\ldots,-1,0,1,\ldots,\frac{n}{2}\}$ or the set $\{-\frac{n}{2},\ldots,-1,0,1,\ldots,\frac{n}{2}-1\}$, while if n is odd, then the complete system of least absolute residues modulo n is the set $\{-\frac{n-1}{2},\ldots,-1,0,1,\ldots,\frac{n-1}{2}\}$. As a result, an integer m belongs to the complete system of least absolute residues modulo n if and only if $|m| \leq \frac{n}{2}$ if n is even, and $|m| \leq \frac{n-1}{2}$ if n is odd.

Lemma 3. *If there exists $j \in \{1,\ldots,n\}$ such that r_{j+1}^{-1} is the least absolute inverse of r_{j+1} modulo r_j, then r_j^{-1} is the least absolute inverse of r_j modulo r_{j-1}.*

Proof. First, we observe that, since $j < n+1$ for every $j = 1,\ldots,n$, we have that $r_j > r_{n+1} = 1$, and thus $r_{j+1}^{-1} \neq 0$; otherwise, $0 \equiv 1 \pmod{r_j}$, whence $r_j|-1$, which contradicts that $r_j > 1$. We note that r_1^{-1} is also nonzero, as a result of $r_0 > 1$. Next, let there exist $j \in \{1,\ldots,n\}$ such that r_{j+1}^{-1} is the least absolute inverse of r_{j+1} modulo r_j. As shown, $r_{j+1}^{-1} \neq 0$, whence $r_{j+1}^{-1} > 0$ or $r_{j+1}^{-1} < 0$. We will examine the two cases separately.

(i) If $r_{j+1}^{-1} > 0$, then, in view of Equation (7),

$$|r_j^{-1}| = \frac{r_{j+1}^{-1}r_{j-1} - 1}{r_j}. \tag{8}$$

Further, since r_{j+1}^{-1} is the least absolute inverse of r_{j+1} modulo r_j, it follows that $r_{j+1}^{-1} \leq \frac{r_j}{2}$ if r_j is even, or $r_{j+1}^{-1} \leq \frac{r_j-1}{2} < \frac{r_j}{2}$ if r_j is odd. Hence, in both cases, $r_{j+1}^{-1} \leq \frac{r_j}{2}$. Multiplying both sides of the last inequality by $\frac{r_{j-1}}{r_j} > 0$ yields $\frac{r_{j+1}^{-1}r_{j-1}}{r_j} \leq \frac{r_{j-1}}{2}$. Next, adding $-\frac{1}{r_j}$ to both sides of the last inequality, we obtain $\frac{r_{j+1}^{-1}r_{j-1}}{r_j} - \frac{1}{r_j} \leq \frac{r_{j-1}}{2} - \frac{1}{r_j} < \frac{r_{j-1}}{2}$, whence $\frac{r_{j+1}^{-1}r_{j-1}-1}{r_j} < \frac{r_{j-1}}{2}$, and in view of Equation (8), we arrive at

$$|r_j^{-1}| < \frac{r_{j-1}}{2}. \tag{9}$$

If r_{j-1} is even, then by Equation (9), the inverse r_j^{-1} belongs to the complete system of least absolute residues modulo r_{j-1}, and since it is an inverse of r_j modulo r_{j-1}, it is the least absolute inverse of r_j modulo r_{j-1}. If r_{j-1} is odd, then there exists an integer k such that $r_{j-1} = 2k+1$, and Equation (9) reads $|r_j^{-1}| < k + \frac{1}{2}$. Next, since $|r_j^{-1}|$ is an integer, the last inequality implies that $|r_j^{-1}| \leq k = \frac{r_{j-1}-1}{2}$, whence $|r_j^{-1}| \leq \frac{r_{j-1}-1}{2}$. Hence, r_j^{-1} belongs to the complete system of least absolute residues modulo r_{j-1}, and since it is an inverse of r_j modulo r_{j-1}, it is the least absolute inverse of r_j modulo r_{j-1}.

(ii) If $r_{j+1}^{-1} < 0$, then in view of Equation (6), we have $j+1 < n+1$, whence $j < n$, and thus $j \leq n-1$, since j is an integer. As a result, $r_j \geq r_{n-1} > r_n > r_{n+1} = 1$, whence $r_j \geq r_{n-1} > r_n > 1$. Consequently, $r_n \geq 2$ and $r_{n-1} \geq 3$, and thus $r_j \geq 3$, whence

$$\frac{1}{r_j} \leq \frac{1}{3}. \tag{10}$$

Besides, in view of Equation (7), we have, since $r_{j+1}^{-1} < 0$,

$$|r_j^{-1}| = \frac{1 - r_{j+1}^{-1} r_{j-1}}{r_j}. \tag{11}$$

Also, as a result of r_{j+1}^{-1} being the least absolute inverse of r_{j+1} modulo r_j, we have that $-r_{j+1}^{-1} \leq \frac{r_j}{2}$ if r_j is even, or $-r_{j+1}^{-1} \leq \frac{r_j - 1}{2} < \frac{r_j}{2}$ if r_j is odd. Hence, in both cases, $-r_{j+1}^{-1} \leq \frac{r_j}{2}$. Multiplying both sides of the last inequality by $\frac{r_{j-1}}{r_j} > 0$ yields $\frac{-r_{j+1}^{-1} r_{j-1}}{r_j} \leq \frac{r_{j-1}}{2}$. Next, adding $\frac{1}{r_j}$ to both sides of the last inequality and taking into account Equation (11), we obtain $|r_j^{-1}| \leq \frac{r_{j-1}}{2} + \frac{1}{r_j}$. Finally, in view of Equation (10), the last inequality gives

$$|r_j^{-1}| \leq \frac{r_{j-1}}{2} + \frac{1}{3}. \tag{12}$$

If r_{j-1} is even, then $\frac{r_{j-1}}{2}$ is an integer, and since $|r_j^{-1}|$ is also an integer, Equation (12) yields $|r_j^{-1}| \leq \frac{r_{j-1}}{2}$. Hence, r_j^{-1} belongs to the complete system of least absolute residues modulo r_{j-1}, and since it is an inverse of r_j modulo r_{j-1}, it is the least absolute inverse of r_j modulo r_{j-1}. If r_{j-1} is odd, then there exists an integer k such that $r_{j-1} = 2k+1$, and Equation (12) reads $|r_j^{-1}| \leq k + \frac{1}{2} + \frac{1}{3} < k+1$. Hence, $|r_j^{-1}| < k+1$ (strict inequality), and since $|r_j^{-1}|$ is an integer, the last inequality yields $|r_j^{-1}| \leq k = \frac{r_{j-1}-1}{2}$; i.e., $|r_j^{-1}| \leq \frac{r_{j-1}-1}{2}$. As a result, r_j^{-1} belongs to the complete system of least absolute residues modulo r_{j-1}, and since it is an inverse of r_j modulo r_{j-1}, it is the least absolute inverse of r_j modulo r_{j-1}. The proof is thus complete. □

Corollary 1. *For every $i = 1, \ldots, n+1$, the inverse r_i^{-1} is the least absolute inverse of r_i modulo r_{i-1}.*

Proof. As explained in the beginning of the proof of Lemma 3, we have that all inverses $r_1^{-1}, \ldots, r_{n+1}^{-1}$ are nonzero. Hence, by Equation (6), we see that r_{n+1}^{-1} is the least absolute inverse of r_{n+1} modulo r_n. By successive application of Lemma 3, we derive that r_i^{-1} is the least absolute inverse of r_i modulo r_{i-1} for every $i = 1, \ldots, n$. □

Remark 3. The reader may easily verify that in Example 1, each of the inverses $r_1^{-1}, \ldots, r_6^{-1}$ is the least absolute inverse.

Lemma 4. *The pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is such that the coefficient of m is the least absolute inverse of $\frac{m}{\gcd(m,n)}$ modulo $\frac{n}{\gcd(m,n)}$, and likewise, the coefficient of n is the least absolute inverse of $\frac{n}{\gcd(m,n)}$ modulo $\frac{m}{\gcd(m,n)}$.*

Proof. Since $m = r_0 \gcd(m, n)$ and $n = r_1 \gcd(m, n)$, the equations of the Euclidean algorithm for m and n result from those for r_0 and r_1; i.e., from the system of Equations (4), if each remainder is multiplied by $\gcd(m, n)$ and each quotient remains unchanged. Since the quotients do not change, the pair of Bézout coefficients does not change either; i.e., the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is equal to the pair of Bézout coefficients that is provided by the Euclidean algorithm for (r_0, r_1). Besides, for $i = 1$, Equation (5) yields that (r_2^{-1}, r_1^{-1}) is the pair of Bézout coefficients that is provided by the Euclidean algorithm for (r_0, r_1). Further, by Corollary 1, the inverse r_2^{-1} is the least absolute inverse of r_2 modulo r_1 and the inverse r_1^{-1} is the least absolute inverse of r_1 modulo r_0. Also, for $i = 1$, Equation (4) reads $r_0 = q_1 r_1 + r_2$, whence $r_0 \equiv r_2 \pmod{r_1}$. Further, both r_0 and r_2 are coprime to r_1, and thus they are both invertible modulo r_1. Hence, the last congruence implies that r_0 and r_2 have the same inverses modulo r_1. As a result, the least absolute inverse of r_2 modulo r_1 is equal to the least absolute inverse of r_0 modulo r_1. Thus, the pair (r_2^{-1}, r_1^{-1}) of Bézout coefficients that is provided by the Euclidean algorithm for (r_0, r_1) is such that the coefficient r_2^{-1} of r_0 is equal to the least absolute inverse of r_0 modulo r_1 and the coefficient r_1^{-1} of r_1 is equal to the least absolute inverse of r_1 modulo r_0. Further, since the pair of Bézout coefficients for (m, n) is equal to that for (r_0, r_1), we conclude that the coefficient of m is equal to r_2^{-1} and the coefficient of n is equal to r_1^{-1}. Therefore, the coefficient of m is the least absolute inverse of $r_0 = \frac{m}{\gcd(m,n)}$ modulo $r_1 = \frac{n}{\gcd(m,n)}$ and the coefficient of n is the least absolute inverse of $r_1 = \frac{n}{\gcd(m,n)}$ modulo $r_0 = \frac{m}{\gcd(m,n)}$. □

Lemma 5. *The pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is such that each coefficient is least in absolute value.*

Proof. Since r_0 and r_1 are coprime, it follows from Lemma 1 that every pair of Bézout coefficients for (r_0, r_1) is such that the coefficient of r_0 is an inverse of r_0 modulo r_1, and likewise, the coefficient of r_1 is an inverse of r_1 modulo r_0. As a result, the absolute value of the coefficient of r_0 is no less than the absolute value of the least absolute inverse of r_0 modulo r_1, and likewise, the absolute value of the coefficient of r_1 is no less than the absolute value of the least absolute inverse of r_1 modulo r_0. Further, as explained in Lemma 4, the pair of Bézout coefficients that is provided by the Euclidean algorithm for (r_0, r_1), say (x_0, y_0), is such that x_0 is the least absolute inverse of r_0 modulo r_1 and y_0 is the least absolute inverse of r_1 modulo r_0. Consequently, the pair (x_0, y_0) is such that each coefficient is least in absolute value. Next, it is easily seen that if (x, y) is a pair of Bézout coefficients for (r_0, r_1), then (x, y) is also a pair of Bézout coefficients for (m, n), and vice versa. As a result, the pair (x_0, y_0) is a pair of Bézout coefficients for (m, n), too, and each coefficient is least in absolute value. Finally, as explained in Lemma 4, the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is equal to the pair of Bézout coefficients that is provided by the Euclidean algorithm for (r_0, r_1). As a result, the pair (x_0, y_0) is the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n). Therefore, the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is such that each coefficient is least in absolute value. □

Corollary 2. *The pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is, as a point in the plane, nearest to the origin.*

Proof. Let (x, y) be the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) and let (x', y') be any pair of Bézout coefficients for (m, n). By Lemma 5, we have $|x| \le |x'|$ and $|y| \le |y'|$. Squaring both sides of both inequalities, adding the two resulting inequalities, and taking square roots on both sides of the resulting inequality, we obtain $\sqrt{x^2 + y^2} \le \sqrt{(x')^2 + (y')^2}$. Therefore, the point (x, y) is nearest to the origin. □

As explained in Lemma 4, the pair of Bézout coefficients that is provided by the Euclidean algorithm for (m, n) is equal to (r_2^{-1}, r_1^{-1}), where r_2^{-1} is equal to the least absolute inverse of r_0 modulo r_1 and r_1^{-1} is equal to the least absolute inverse of r_1 modulo r_0. As a result, r_2^{-1} belongs to the complete system of least absolute residues modulo r_1 and r_1^{-1} belongs to the complete system of least absolute residues modulo r_0. Since r_0 and r_1 are coprime, they cannot be both even. As a result, r_0 and r_1 are both odd, r_0 is odd and r_1 is even, or r_0 is even and r_1 is odd. In the first case, we have $|r_1^{-1}| \le \frac{r_0-1}{2}$ and $|r_2^{-1}| \le \frac{r_1-1}{2}$, in the second case, we have $|r_1^{-1}| \le \frac{r_0-1}{2}$ and $|r_2^{-1}| \le \frac{r_1}{2}$, and in the third case, we have $|r_1^{-1}| \le \frac{r_0}{2}$ and $|r_2^{-1}| \le \frac{r_1-1}{2}$. The previous bounds slightly improve those given by Rankin [6, Proposition 1]. Now, squaring each of the previous three pairs of inequalities and adding, each time, the two resulting inequalities, we obtain $(r_1^{-1})^2 + (r_2^{-1})^2 \le \frac{(r_0-1)^2+(r_1-1)^2}{4}$, $(r_1^{-1})^2 + (r_2^{-1})^2 \le \frac{(r_0-1)^2+r_1^2}{4}$, and $(r_1^{-1})^2 + (r_2^{-1})^2 \le \frac{r_0^2+(r_1-1)^2}{4}$, respectively. Hence, in the plane, the point (r_2^{-1}, r_1^{-1}) lies in the interior of the circle or on the circle centered at the origin with radius $\frac{\sqrt{(r_0-1)^2+(r_1-1)^2}}{2}$, $\frac{\sqrt{(r_0-1)^2+r_1^2}}{2}$, and $\frac{\sqrt{r_0^2+(r_1-1)^2}}{2}$, respectively. Further, the point (r_2^{-1}, r_1^{-1}) is unique, as a result of the modular inverse being unique with respect to the modulus.

Next, we will show that if r_0 and r_1 are both odd or if r_0 is odd and r_1 is even, then the previous bounds on r_1^{-1} and r_2^{-1} cannot be sharpened, while if r_0 is even and r_1 is odd, then they can. We note that $r_0 > r_1 > 1$.

Lemma 6. *Let r_0 and r_1 be both odd. It holds that $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1-1}{2}$ if and only if $r_0 - r_1 = 2$.*

Proof. We assume that $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1-1}{2}$. By Equation (5) for $i = 1$, we have $1 = r_2^{-1}r_0 + r_1^{-1}r_1$, and since r_0 and r_1 are both positive, it follows that r_1^{-1} and r_2^{-1} have different signs. If $r_1^{-1} = -\frac{r_0-1}{2}$ and $r_2^{-1} = \frac{r_1-1}{2}$, then $1 = \frac{r_1-1}{2}r_0 - \frac{r_0-1}{2}r_1 = \frac{r_1-r_0}{2} < 0$, which is a contradiction. If $r_1^{-1} = \frac{r_0-1}{2}$ and $r_2^{-1} = -\frac{r_1-1}{2}$, then $1 = \frac{r_0-r_1}{2}$, whence $r_0 - r_1 = 2$.

Next, we assume that $r_0 - r_1 = 2$. Since r_0 and r_1 are both odd, we have $r_0 = 2k+1$ and $r_1 = 2(k-1)+1$, for some integer $k > 1$. Applying the Euclidean algorithm to r_0 and r_1 yields

$$r_0 = 1 \cdot r_1 + 2,$$

$$r_1 = (k-1) \cdot 2 + 1.$$

Hence, we have

$$1 = r_1 - (k-1) \cdot 2 = r_1 - (k-1) \cdot (r_0 - r_1) = -(k-1)r_0 + kr_1;$$

that is, $-(k-1)r_0 + kr_1 = 1$, and since $k = \frac{r_0-1}{2}$ and $k - 1 = \frac{r_1-1}{2}$, we have $-\frac{r_1-1}{2}r_0 + \frac{r_0-1}{2}r_1 = 1$. Finally, comparing the last equation with Equation (5) for $i = 1$, we arrive at $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1-1}{2}$. □

We remark that if r_0 and r_1 are both odd, then, taking into account that $r_0 > r_1$, we have $r_0 - r_1 \geq 2$. If, additionally, $r_0 - r_1 > 2$, then, by Lemma 6, at least one of the inequalities $|r_1^{-1}| \leq \frac{r_0-1}{2}$ and $|r_2^{-1}| \leq \frac{r_1-1}{2}$ is strict.

Lemma 7. *Let r_0 be odd and r_1 be even. It holds that $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1}{2}$ if and only if $r_1 = 2$.*

Proof. We assume that $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1}{2}$. By Equation (5) for $i = 1$, we have $1 = r_2^{-1}r_0 + r_1^{-1}r_1$, and since r_0 and r_1 are both positive, it follows that r_1^{-1} and r_2^{-1} have different signs. If $r_1^{-1} = \frac{r_0-1}{2}$ and $r_2^{-1} = -\frac{r_1}{2}$, then $1 = -\frac{r_1}{2}r_0 + \frac{r_0-1}{2}r_1 = -\frac{r_1}{2} < 0$, which is a contradiction. If $r_1^{-1} = -\frac{r_0-1}{2}$ and $r_2^{-1} = \frac{r_1}{2}$, then $1 = \frac{r_1}{2}$, whence $r_1 = 2$.

Next, we assume that $r_1 = 2$. Since $r_0 > r_1$ and r_0 is odd, it follows that $r_0 = 2k + 1$, for some positive integer k. As a result, $r_0 = kr_1 + 1$, and thus $r_0 - kr_1 = 1$. Comparing the last equation with Equation (5) for $i = 1$, we obtain $r_2^{-1} = 1 = \frac{r_1}{2}$ and $r_1^{-1} = -k = -\frac{r_0-1}{2}$, whence $|r_1^{-1}| = \frac{r_0-1}{2}$ and $|r_2^{-1}| = \frac{r_1}{2}$. □

As a consequence of Lemma 7, if r_0 is odd and r_1 is even and greater than 2, then at least one of the inequalities $|r_1^{-1}| \leq \frac{r_0-1}{2}$ and $|r_2^{-1}| \leq \frac{r_1}{2}$ is strict.

Lemma 8. *If r_0 is even and r_1 is odd, then at least one of the inequalities $|r_1^{-1}| \leq \frac{r_0}{2}$ and $|r_2^{-1}| \leq \frac{r_1-1}{2}$ is strict.*

Proof. Suppose to the contrary that none of the two given inequalities is strict. As a result, there exist r_0 and r_1 such that $|r_1^{-1}| = \frac{r_0}{2}$ and $|r_2^{-1}| = \frac{r_1-1}{2}$. By Equation (5) for $i = 1$, we have $1 = r_2^{-1}r_0 + r_1^{-1}r_1$, and since r_0 and r_1 are both positive, it follows that r_1^{-1} and r_2^{-1} have different signs. As a result, $r_1^{-1} = \frac{r_0}{2}$ and $r_2^{-1} = -\frac{r_1-1}{2}$, or $r_1^{-1} = -\frac{r_0}{2}$ and $r_2^{-1} = \frac{r_1-1}{2}$. In the first case, we have $1 = -\frac{r_1-1}{2}r_0 + \frac{r_0}{2}r_1 = \frac{r_0}{2}$, whence $r_0 = 2$, and thus $2 > r_1 > 1$, which is a contradiction, since r_1 is an integer. In the second case, we have $1 = -\frac{r_0}{2} < 0$, which is a contradiction, too. □

Remark 4. As a consequence of Lemma 8, if r_0 is even and r_1 is odd, then the point (r_2^{-1}, r_1^{-1}) lies in the interior of the circle centered at the origin with radius $\frac{\sqrt{r_0^2+(r_1-1)^2}}{2}$.

Acknowledgement. The author is grateful to the anonymous referee for valuable remarks and suggestions.

References

[1] S. P. Glasby, Extended Euclid's algorithm via backward recurrence relations, *Math. Mag.* **72** (1999), 228–230.

[2] Z. Hu, I. A. Dychka, O. Mykola, and B. Andrii, The analysis and investigation of multiplicative inverse searching methods in the ring of integers modulo m, *I.J. Intelligent Systems and Applications* **8** (2016), 9–18.

[3] T. Jebelean, An algorithm for exact division, *J. Symbolic Comput.* **15** (1993), 169–180.

[4] M. Joye and P. Paillier, GCD-free algorithms for computing modular inverses, in *Cryptographic Hardware and Embedded Systems-CHES 2003: 5th International Workshop, Cologne, Germany, September 8–10*, Springer, Berlin, Heidelberg, 2003.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., New York, 1991.

[6] S. A. Rankin, The Euclidean algorithm and the linear Diophantine equation $ax+by = \gcd(a, b)$, *Amer. Math. Monthly* **120** (2013), 562–564.

[7] K. H. Rosen, *Elementary Number Theory and Its Applications*, Pearson, London, 2011.