Functiones et Approximatio
XXVIII (2000), 221–232

Dedicated to Professor Włodzimierz Staś
on his 75th birthday

ON THE COMMON FACTORS OF $2^N - 3$ AND $3^N - 2$

KAZIMIERZ SZYMICZEK

Abstract: We prove that there are infinitely many natural numbers n for which the greatest common divisor of $2^n - 3$ and $3^n - 2$ is divisible by 26665.

1. Introduction

A curious problem on the common factors of the numbers $2^n - 3$ and $3^n - 2$ was proposed by A. Schinzel in 1997. He asked for an argument rejecting the unlikely statement that for sufficiently large primes p the number $2^n - 3$ is divisible by p if and only if $3^n - 2$ is divisible by p. This has been resolved by G. Banaszak (see [1]) who constructed an infinite sequence of natural numbers $n_1, n_2, \dots$ with the property that the number $2^{n_k} - 3$ has a large prime divisor which does not divide the number $3^{n_k} - 2$. While this solves the Schinzel problem it only whets the appetite for more precise information on the common prime factors of the numbers $2^n - 3$ and $3^n - 2$. Clearly the ultimate question is to find the greatest common divisor of the numbers $2^n - 3$ and $3^n - 2$ for all n.

Using the GP/Pari calculator one immediately encounters a pattern of values which seems to be a rule. The result is that for all $n \leq 3000$,

$$\gcd(2^n - 3, 3^n - 2) = \begin{cases} 1 & \text{if } n \equiv 0, 1, 2 \bmod 4, \\ 5 & \text{if } n \equiv 3 \bmod 4. \end{cases} \tag{1.1}$$

However, it is surprising that pushing the calculations a bit further one arrives at

$$\gcd(2^{3783} - 3, 3^{3783} - 2) = 26665 = 5 \cdot 5333 \tag{1.2}$$

instead of the expected value 5. We are far from understanding that phenomenon but in this note we do three things. First, although we are unable to prove that the greatest common divisor in (1.2) *equals* 26665, we show how to verify that

$$26665 \mid \gcd(2^{3783} - 3, 3^{3783} - 2). \tag{1.3}$$

Actually we will give several proofs for that. Second, we prove that there are infinitely many exceptions to the rule (1.1). In all of them the gcd is divisible by

26665. We find all exponents n for which the latter holds. Third, we report on computer calculations establishing some bounds for n where no new phenomena occur. Also we discuss the common divisors of $a^n - b$ and $b^n - a$ for $(a, b) = (2,5), (2,7), (3,5), (3,7), (5,7)$ and find that their behaviour is pretty close to the case $a = 2, b = 3$.

The main purpose of this paper is to *prove* the unexpected numerical phenomenon (1.3) found by computer calculations. Computer findings do not qualify as proofs, at least to some authors who think that *perhaps rodents in the bowels of the computer center are chewing on wires and altering data* (see [2]). While in our case the computers we have used have been under full control and rodents have been nowhere in sight, the smaller computer animals like bugs and viruses are likely to inhabit some machines. So we definitely need a proof for (1.3).

2. Three observations

We collect here three simple facts on the regularity of appearance of divisors of the numbers $a^n - b$. We are interested mainly in the cases when $a = 2, b = 3$ or $a = 3, b = 2$ but the general case is as simple as these special cases. So we fix two coprime positive integers $a > 1$ and $b > 1$ and an odd prime p. Let us denote by $\ell_p(a)$ the exponent to which a belongs mod$p$, or in other words, the order of the residue class $a \bmod p$ in the multiplicative group of the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus $\ell_p(a) \,|\, p-1$.

Theorem 2.1. *Let n and m be natural numbers and assume that $p \,|\, a^m - b$. Then*

$$p \,|\, a^n - b \iff n \equiv m \pmod{\ell_p(a)}.$$

Proof. Assume first that $p \,|\, a^n - b$ and, say, $n > m$. Then we have

$$p|(a^n - b) - (a^m - b) = a^m(a^{n-m} - 1).$$

Since a and p are coprime it follows that $n \equiv m \pmod{\ell_p(a)}$.

On the other hand, if $n \equiv m \pmod{\ell_p(a)}$ and $n > m$ say, then $n = m + d\ell_p(a)$ for a nonnegative integer d. Now we have

$$a^n - b = a^m(a^{d\ell_p(a)} - 1) + a^m - b.$$

Hence, since $p \,|\, a^m - b$, it follows that $p \,|\, a^n - b$. ■

Theorem 2.2. *Suppose there is a natural number n such that*

$$p \,|\, a^n - b \quad \text{and} \quad p \,|\, b^n - a. \tag{2.1}$$

Then $\ell_p(a) = \ell_p(b) =: \ell$, and $\ell \,|\, n^2 - 1$. Moreover, for the smallest n satisfying (2.1) the following holds

$$n < \ell < p \quad .$$

Proof. Write A and B for the residue classes of $a \pmod p$ and $b \pmod p$, respectively. If (2.1) is satisfied, then we have

$$A^n = B \quad \text{and} \quad B^n = A \tag{2.2}$$

in the multiplicative group $\mathbb{F}_p^*$. Hence B belongs to the cyclic subgroup $\langle A\rangle$ generated by A, and A belongs to the cyclic subgroup $\langle B\rangle$ generated by B. It follows that $\langle A\rangle = \langle B\rangle$, hence also

$$\ell_p(a) = \#\langle A\rangle = \#\langle B\rangle = \ell_p(b).$$

Moreover, from (2.2) we get $A^{n^2} = B^n = A$, whence $\ell_p(a)\,|\,n^2-1$.

If n is the smallest nonnegative integer such that $A^n = B$, then A^n is one of the elements $A^0, A^1, \dots, A^{\ell-1}$ of the group $\langle A\rangle$, hence $0 \le n < \ell$. ■

Theorem 2.3. *If $p\,|\,a^n-b$, then*

$$p\,|\,b^n-a \iff \ell_p(a)\,|\,n^2-1.$$

Proof. Assume first that $p\,|\,a^n-b$ and $\ell_p(a)\,|\,n^2-1$. Using the notation of the previous proof, we have $A^n = B$ and $A^{n^2-1} = 1$ in $\mathbb{F}_p$. Hence also

$$B^n = A^{n^2} = A,$$

as required. The other part has already been proved in Theorem 2.2. ■

3. Direct proof

Here we show how to verify (1.3) without using any computer aided calculations. So we are to show that for $n = 3783$ the greatest common divisor of 2^n-3 and 3^n-2 is divisible by the primes 5 and 5333. The first part is easy for we have the following result.

Lemma 3.1. *For a natural number n,*

$$5\,|\,\gcd(2^n-3, 3^n-2) \iff n \equiv 3 \pmod 4.$$

Proof. We have $\ell_5(2) = \ell_5(3) = 4$ and $5\,|\,\gcd(2^3-3, 3^3-2)$. Hence taking $m = 3$ and $p = 5$, the result follows from Theorem 2.1. ■

The second part is more involved although the result is quite similar to that of Lemma 3.1.

Lemma 3.2. *For a natural number n,*

$$5333 \mid \gcd(2^n - 3, 3^n - 2) \iff n \equiv 3783 \pmod{5332}.$$

Proof. We will prove the assertion in two steps.

Step 1. $5333 \mid 2^{3783} - 3$.

First observe that $p = 5333 \equiv 5 \pmod{8}$ so that 2 is a quadratic non-residue mod$p$. It follows that in $\mathbb{F}_p$,

$$2^{2666} = 2^{(p-1)/2} = -1.$$

Hence

$$2^{3783} = 2^{2666+1117} = -2^{1117}$$

and the desired equality $2^{3783} = 3$ is equivalent to

$$2^{1117} = -3 \quad \text{in} \quad \mathbb{F}_p. \tag{3.1}$$

So in the original problem the exponent $n = 3783$ is in the upper half of the interval $[1, p-1]$, and in the reduced problem (3.1) the exponent lies in the lower half of the interval $[1, p-1]$. In principle the problem becomes easier.

We use a well known method of computing the residue $a^k \pmod{m}$ (see, for instance, [5], p. 126), the *successive squaring* method. So first we write the exponent 1117 as the sum of 2−powers,

$$1117 = 2^{10} + 2^6 + 2^4 + 2^3 + 2^2 + 1,$$

so that

$$2^{1117} = 2^{2^{10}} \cdot 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^3} \cdot 2^{2^2} \cdot 2^1.$$

Next calculate the residues of $2^{2^i} \pmod{5333}$.

$$2^1 \equiv 2, \quad 2^{2^1} \equiv 4, \quad 2^{2^2} \equiv 16, \quad 2^{2^3} \equiv 256,$$

$$2^{2^4} \equiv 256^2 \equiv 1540,$$

$$2^{2^5} \equiv 1540^2 \equiv 3748,$$

$$2^{2^6} \equiv 3748^2 \equiv 382,$$

$$2^{2^7} \equiv 382^2 \equiv 1933,$$

$$2^{2^8} \equiv 1933^2 \equiv 3389,$$

$$2^{2^9} \equiv 3389^2 \equiv 3372,$$

$$2^{2^{10}} \equiv 3372^2 \equiv 428.$$

Now we compute the residue of $2^{1117} \pmod{5333}$ as follows. For brevity, write

$$A_3 := 2^{2^3} \cdot 2^{2^2} \cdot 2^1, \quad A_4 := 2^{2^4} \cdot A_3, \quad A_6 := 2^{2^6} \cdot A_4, \quad A_{10} := 2^{2^{10}} \cdot A_6 = 2^{1117}.$$

Then we get

$$\begin{aligned} A_3 &= 256 \cdot 16 \cdot 2 = 5333 \cdot 1 + 2859 \equiv 2859, \\ A_4 &\equiv 1540 \cdot 2859 = 5333 \cdot 825 + 3135 \equiv 3135, \\ A_6 &\equiv 382 \cdot 3135 = 5333 \cdot 224 + 2978 \equiv 2978, \\ A_{10} &\equiv 428 \cdot 2978 = 5333 \cdot 238 + 5330 \equiv -3. \end{aligned}$$

This proves the asserted equality (3.1) and finishes the Step 1.

Step 2. $5333 \,|\, 2^{3783} - 3$ and $5333 \,|\, 3^{3783} - 2$.

In view of Theorem 2.3 the divisibility $p \,|\, 3^{3783} - 2$ follows from the fact that $p \,|\, 2^{3783} - 3$ and $p - 1 \,|\, 3783^2 - 1$. The first divisibility has been established in Step 1 and the second divisibility is easily checked.

We are going to use the fact that $\ell_p(2) = p - 1$. This is proved in the next section (see Proposition 4.1). With this, the equivalence statement in Lemma 3.2 follows from Theorem 2.1 and from Step 2. ■

Example 3.3. We could have attacked the problem directly trying to calculate the residue of 2^{3783} mod 5333. Observe that

$$3783 = 2^{11} + 2^{10} + 2^9 + 2^7 + 2^6 + 2^2 + 2^1 + 2^0$$

Hence

$$2^{3783} = 2^{2^{11}} \cdot 2^{2^{10}} \cdot 2^{2^9} \cdot 2^{2^7} \cdot 2^{2^6} \cdot 2^{2^2} \cdot 2^{2^1} \cdot 2^{2^0}$$

and so we would have to compute the residues of 2^{2^i} up to $i = 11$ and then proceed as above. These computations require more steps and also higher exponents occur than in the approach we have applied.

Example 3.4. For further reference we want to establish that

$$2^{117} \equiv 3^{55} \pmod{5333}.$$

This can be done by using the successive squaring method. So we write $117 = 2^6 + 2^5 + 2^4 + 5$ and $55 = 2^5 + 2^4 + 7$ and then we use the already computed residues of 2^{2^i} modulo $p = 5333$. So we get

$$2^{117} = 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^4} \cdot 2^5 \equiv 382 \cdot 3748 \cdot 1540 \cdot 32 \equiv 2769 \pmod{p}.$$

Similarly, computing the residues of 3^{2^i} modulo p we get

$$3^{55} = 3^{2^5} \cdot 3^{2^4} \cdot 3^7 \equiv 1790 \cdot 4078 \cdot 2187 \equiv 2769 \pmod{p}.$$

This establishes the claim. However, it is interesting to notice that we also have

$$3^{117} \equiv 2^{55} \pmod{5333}.$$

We prove this in a slightly more general setting. We assert that for any natural numbers n, m,

$$2^n \equiv 3^m \pmod{5333} \iff 3^n \equiv 2^m \pmod{5333}.$$

To prove this we use two facts, first $2^{3783} = 3$ and $3^{3783} = 2$ in $\mathbb{F}_p$, and second, $\ell_p(2) = \ell_p(3) = p - 1$, proved in the next section (see Proposition 4.1). Then we have in $\mathbb{F}_p$,

$$\begin{aligned} 2^n = 3^m &\iff 2^n = 2^{3783m} \iff n \equiv 3783m \pmod{p-1} \\ &\iff 3^n = 3^{3783m} \iff 3^n = 2^m. \end{aligned}$$

4. Other direct proofs

Here we give several other proofs of the fact that 5333 is a common factor of $2^{3783} - 3$ and $3^{3783} - 2$. As remarked in Step 2 of the proof of Lemma 3.2, it is sufficient to establish that for $p = 5333$ and $n = 3783$ either $p \mid 2^n - 3$ or $p \mid 3^n - 2$. Throughout this section we set $p = 5333$.

Preliminaries. Here we establish several identities in the multiplicative group $\mathbb{F}_p^*$. We start with some obvious decompositions in $\mathbb{Z}$:

$$p = 2^2 \cdot 11^3 + 3^2, \quad p + 2 \cdot 3^5 = 11 \cdot 23^2, \quad p + 2^8 = 3^5 \cdot 23.$$

Thus we get in $\mathbb{F}_p$:

$$2^2 \cdot 11^3 = -3^2, \quad 2 \cdot 3^5 = 11 \cdot 23^2, \quad 2^8 = 3^5 \cdot 23. \tag{4.1}$$

The third identity squared becomes $2^{16} = 3^{10} \cdot 23^2$, and now eliminating 23^2 we obtain $2^{16} \cdot 11 = 2 \cdot 3^{15}$ or $2^{15} \cdot 11 = 3^{15}$. Now raising the first identity in (4.1) to the power 8 we get $2^{16} \cdot 11^{24} = 3^{16}$ and combining with $2^{15} \cdot 11 = 3^{15}$ we arrive at the nontrivial relation

$$2 \cdot 11^{23} = 3 \quad \text{in} \quad \mathbb{F}_p. \tag{4.2}$$

Observe that we could have used once more the method of successive squaring to compute the residue of $11^{23} \pmod{p}$. For $23 = 2^4 + 2^2 + 3$ and computing the residues modulo $p = 5333$ we get

$$11^{23} = 11^{2^4} \cdot 11^{2^2} \cdot 11^3 \equiv 1652 \cdot 3975 \cdot 1331 \equiv 1652 \cdot 389 \equiv 2668 \pmod{p}.$$

Hence $2 \cdot 11^{23} \equiv 2 \cdot 2668 \equiv 3 \pmod{p}$.

The identity (4.2) has several interesting consequences. First we get $2^2 \cdot 11^{46} = 3^2$ which combined with $2^2 \cdot 11^3 = -3^2$ gives

$$11^{43} = -1.$$

It follows that $\ell_p(11) = 86$. This is the only instance among small primes where the prime belongs mod p to a small exponent. Using GP/Pari calculator one can check that primes like $2, 3, 5, 7, 17, 19, 23, 29$ all are primitive roots modulo p, and 13 belongs to 2666 mod p. We will give below a direct proof that 2 and 3 are primitive roots mod$p$. Another consequence of (4.2) is

$$2^{43} = -3^{43} \quad \text{in} \quad \mathbb{F}_p. \tag{4.3}$$

This can be obtained by raising the identity (4.2) to the power 43 and using $11^{43} = -1$.

Now we show that $\ell_p(6) = 31$. For this it is sufficient to prove that

$$6^{31} = 1 \quad \text{in} \quad \mathbb{F}_p. \tag{4.4}$$

This follows immediately from the identities

$$11 \cdot 17 \cdot 2^{15} = -1 \quad \text{and} \quad 17 \cdot 3^{15} = -1 \quad \text{in} \quad \mathbb{F}_p. \tag{4.5}$$

Indeed, squaring and multiplying the two identities we get

$$11^2 \cdot 17^4 \cdot 6^{30} = 1,$$

so it remains to show that $11^2 \cdot 17^4 = 6$ in $\mathbb{F}_p$. This involves manipulations with 4-digit integers and for completeness we include the (trivial) details. So we have

$$\begin{aligned} 11^2 \cdot 17 &= 2057, \\ 11^2 \cdot 17^2 &= 2057 \cdot 17 \equiv 2971 \pmod{p}, \\ 11^2 \cdot 17^3 &\equiv 2971 \cdot 17 \equiv 2510 \pmod{p}, \\ 11^2 \cdot 17^4 &\equiv 2510 \cdot 17 \equiv 6 \pmod{p}. \end{aligned}$$

It remains to establish the identities (4.5). We start with the observation

$$3p = 5^6 + 2 \cdot 11 \cdot 17 \quad \text{and} \quad 3p + 1 = 2^7 \cdot 5^3.$$

Thus we have $-5^6 = 2 \cdot 11 \cdot 17$ and $2^7 \cdot 5^3 = 1$ in $\mathbb{F}_p$. Squaring the second and combining with the first gives the first identity in (4.5). The second can be derived from the first and from (4.2). For the latter implies $2^{15} \cdot (11^{23})^{15} = 3^{15}$, and since $23 \cdot 15 \equiv 1 \pmod{86}$, we get $2^{15} \cdot 11 = 3^{15}$. Now the second identity in (4.5) follows from the first. This finishes the proof of $6^{31} = 1$.

Before we prove that 2 and 3 are primitive roots $\pmod p$ we must establish two more identities in $\mathbb{F}_p$. These are

$$2^{62} = 11^{61} \quad \text{and} \quad 3^{62} = 11^{25}. \tag{4.6}$$

Observe that $p-1 = 62 \cdot 86$, hence $(2^{62})^{86} = 1$ and $(3^{62})^{86} = 1$ in $\mathbb{F}_p$. The cyclic group $\mathbb{F}_p^*$ has only one subgroup of order 86 and this is generated by 11. Thus we must have $2^{62} = 11^a$ and $3^{62} = 11^b$ for certain positive integers $a, b \leq 86$. Actually, we have $a = 61$ and $b = 25$ and that is what we are going to prove.

From (4.2) we have $2^2 \cdot 11^{23} = 6$, hence $2^{62} \cdot (11^{23})^{31} = 6^{31}$. By (4.4) and $23 \cdot 31 \equiv 25 \pmod{86}$ we get

$$2^{62} \cdot 11^{25} = 1.$$

Multiplying this by 11^{61} and using $11^{86} = 1$ we get the first identity in (4.6). And multiplying the last displayed identity by 3^{62} we get $6^{62} \cdot 11^{25} = 3^{62}$ which combined with (4.4) gives the second identity in (4.6). A further piece of information is provided by the following result.

Proposition 4.1. 2 *and* 3 *are primitive roots* mod5333.

Proof. We prove only that $\ell_p(2) = p-1$ since the other part of the proof is quite similar. Notice that $p-1 = 4 \cdot 31 \cdot 43$ so that it is sufficient to show that $\ell_p(2)$ is divisible by $4, 31$ and 43. We will use the following simple principle: for any natural number k, we have $\ell_p(2^k) \mid \ell_p(2)$.

Step 1. $4 \mid \ell_p(2)$.

We know that $2^{(p-1)/2} = -1$ in $\mathbb{F}_p$, hence $\ell_p(2^{(p-1)/4}) = 4$. By the principle, $4 \mid \ell_p(2)$.

Step 2. $31 \mid \ell_p(2)$.

We use the already proved fact that $2^n = 3$ in $\mathbb{F}_p$ for $n = 3783$ (see Step 1 in Lemma 3.2). Thus we have $2^{n+1} = 6 \neq 1$ and since $n+1 = 172 \cdot 22$ it follows that $2^{172} \neq 1$. On the other hand $p-1 = 172 \cdot 31$ so that $2^{172} = 2^{(p-1)/31} \neq 1$. It follows that $\ell_p(2^{172}) = 31$, and so 31 divides $\ell_p(2)$.

Step 3. $43 \mid \ell_p(2)$.

We know that $\ell_p(11) = 86$ and since $\gcd(61, 86) = 1$, also $\ell_p(11^{61}) = 86$. Hence, by (4.6), we have $\ell_p(2^{62}) = 86$ and so $86 \mid \ell_p(2)$. ∎

Second proof. This is based on the equality $6^{31} = 1$ in $\mathbb{F}_p$ (see (4.4)). Set $n = 3783$. From (4.2) we get

$$2^{n+1} \cdot \left(11^{23}\right)^{n+1} = 3^{n+1},$$

But $n+1 = 2^3 \cdot 11 \cdot 43$ is divisible by 86, the order of 11 in the group $\mathbb{F}_p$, hence $2^{n+1} = 3^{n+1}$. In $\mathbb{F}_p$ write a for the common value of $2^n \cdot 3^{-1}$ and $3^n \cdot 2^{-1}$. Then

$$2^n = 3a \quad \text{and} \quad 3^n = 2a \tag{4.7}$$

and it remains to show that $a = 1$. First we show that $a^{43} = 1$. Using (4.3), we have

$$2^{43n} = 3^{43} \cdot a^{43} = -2^{43} \cdot a^{43},$$

hence $2^{43(n-1)} = -a^{43}$. But $43(n-1) = (p-1)/2 \cdot 61$, so we get

$$-1 = (-1)^{61} = \left(2^{(p-1)/2}\right)^{61} = -a^{43}.$$

Hence $a^{43} = 1$.

The second step is to show that $a^2 = 1$. From (4.7) we get $6^n = 6a^2$ and so $6^{n-1} = a^2$. On the other hand $31 \mid n-1$ and $6^{31} = 1$, so it follows that $1 = 6^{n-1} = a^2$.

Clearly $a^{43} = 1$ and $a^2 = 1$ give $a = 1$. Hence $2^n = 3$, as desired.

Third proof. Here we will use the equality $2^{55} = 3^{117}$ in $\mathbb{F}_p$ established in Example 3.4. Observe that

$$3783 \equiv 55 \cdot 5013 \pmod{p-1} \quad \text{and} \quad 117 \cdot 5013 \equiv 1 \pmod{p-1}.$$

Thus raising $2^{55} = 3^{117}$ to the power 5013 we get in $\mathbb{F}_p$

$$2^{3783} = (2^{55})^{5013} = (3^{117})^{5013} = 3.$$

It is interesting to notice that the equality $2^{55} = 3^{117}$ can also be established by using the identities (4.2) and (4.6). Indeed, by the latter, $3^{124} = 11^{50}$, and by (4.2) we have $3^7 = 11^{75} \cdot 2^7$. Combining these we get

$$3^{117} = 11^{-25} \cdot 2^{-7} = 11^{61} \cdot 2^{-7} = 2^{55},$$

the latter by (4.6).

Fourth proof. Observe that $3783 = 61^2 + 61 + 1$, and by (4.6) we have $3^{61} \cdot 3 = 11^{25}$. This gives

$$3^{61^2} \cdot 3^{61} = \left(11^{25}\right)^{61} = 11^{63},$$

since $11^{86} = 1$ and $25 \cdot 61 \equiv 63 \pmod{86}$. Finally

$$3^{3783} = 3^{61^2} \cdot 3^{61} \cdot 3 = 3 \cdot 11^{63} = 2,$$

the latter by the identity (4.2) which is equivalent to $3 \cdot 11^{63} = 2$.

5. There are infinitely many exceptions

We have been directing our effort to prove that the expected pattern of the values of $\gcd(2^n - 3, 3^n - 2)$ breaks down for the value $n = 3783$. But from Lemma 3.2 it follows that, in fact, there are infinitely many exceptions. We describe completely the exponents n for which $26665 = 5 \cdot 5333$ is a common divisor of $2^n - 3$ and $3^n - 2$.

Proposition 5.1. *For a natural number n,*

$$26665 \mid \gcd(2^n - 3, 3^n - 2) \iff n \equiv 3783 \pmod{5332}$$

Proof. Combine the lemmas 3.1 and 3.2. ■

We are unable to prove that the greatest common divisor of $2^n - 3$ and $3^n - 2$ for the values of n specified in the proposition actually equals 26665. However, using the GP/Pari calculator (version 2.0.17 beta) we have computed the $\gcd(2^n - 3, 3^n - 2)$ for 101 consecutive numbers of the form $n = 3783 + 5332x$ ($x = 0, 1, \ldots, 100$), the largest being $n = 536983$. In all cases the gcd equals 26665. (Notice that the number $3^{536983} - 2$ has 256207 decimal digits.)

At the moment, the $\gcd(2^n - 3, 3^n - 2)$ have been computed for all $n \leq 200000$ and the pattern set by (1.1) works all right except for $n \equiv 3783 \pmod{5332}$, where in all cases the gcd equals 26665. The calculations in the range $80000 \leq n \leq 200000$ have been performed on a 500 MHz Pentium III IBM Netfinity 3000 machine. They took 412 hours of computer work.

Remark. If we are interested only in showing that there are infinitely many integers n satisfying $2^n = 3$ and $3^n = 2$ in $\mathbb{F}_p$, then there is an easy and immediate proof that, if this holds for one exponent m, then it holds for infinitely many exponents. For as we have already observed, $2^m = 3$ and $3^m = 2$ imply $2^{m^2} = 3^m = 2$ and $3^{m^2} = 2^m = 3$, hence for any natural number k we have

$$2^{m^{2k}} = 2 \quad \text{and} \quad 3^{m^{2k}} = 3.$$

It follows that

$$2^{m^{2k+1}} = (2^{m^{2k}})^m = 2^m = 3 \quad \text{and} \quad 3^{m^{2k+1}} = (3^{m^{2k}})^m = 3^m = 2.$$

Hence all exponents m^{2k+1} solve our problem if m does.

Notice that this agrees with Lemma 3.2. According to the Lemma we must have $m \equiv 3783 \pmod{p-1}$ and since $3783^2 \equiv 1 \pmod{p-1}$, we have $m^{2k+1} \equiv 3783^{2k+1} \equiv 3783 \pmod{p-1}$. Hence for $n = m^{2k+1}$ we have $p \mid \gcd(2^n-3, 3^n-2)$ by Lemma 3.2.

6. Prime divisors of the numbers $a^n - b$ and $b^n - a$

We continue to assume that $a > 1$ and $b > 1$ are coprime integers. We say that a prime number p is an $(a, b)-$divisor if there exists a natural number n such that

$$p \mid a^n - b \quad \text{and} \quad p \mid b^n - a.$$

Thus, for instance, the primes 5 and 5333 are $(2, 3)-$divisors and we do not know any others.

It is tempting to look at some other values of a and b. Using GP/Pari calculator we have verified (in 450 hours of a modest computer work) that for

$n \leq 50000$ only the following prime numbers occur as $(a, b)-$divisors for $a, b \in \{2, 3, 5, 7\}$.

$5, 5333$	are $(2, 3)$-divisors,
$3, 1031. 1409$	are $(2, 5)$-divisors,
$5, 13, 61, 67, 211, 19423$	are $(2, 7)$-divisors,
$2. 7, 2333, 8537, 13757, 37123$	are $(3, 5)$-divisors,
$2, 5, 79, 300673$	are $(3, 7)$-divisors,
$2, 17. 97, 227251$	are $(5, 7)$-divisors.

Although this evidence is very limited and discouraging we are ready to conjecture that *for any relatively prime natural numbers a, b the set of prime $(a, b)-$ divisors is infinite.*

Clearly, first one would like to know that each sequence $a^n - b$ has infinitely many prime divisors. This however is a well known fact (see, for instance, [4, Aufgabe VIII.107]; I owe this reference to A. Schinzel).

A modern proof runs as follows. Suppose $p_1, \ldots, p_k$ are all prime divisors of the numbers of the form $a^n - b$, where $n \in \mathbb{N}$. Let S be the set of primes consisting of the prime factors of a and of all the $p_1, \ldots, p_k$. We consider the ring $\mathcal{O}$ of $S-$integers in the field $\mathbb{Q}$ of rational numbers. It follows that for any $n \in N$ there are nonnegative integers $\alpha_1, \ldots, \alpha_k$ such that

$$a^n - p_1^{\alpha_1} \cdots p_k^{\alpha_k} = b.$$

Hence with $a_1 = 1/b$ and $a_2 = -1/b$ the equation

$$a_1 x_1 + a_2 x_2 = 1$$

has infinitely many solutions in $S-$units $x_1 = a$ and $x_2 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. This contradicts a well known result of van der Poorten, Schlickewei and Evertse (see [3, p. 19]).

Another conjecture we want to make goes in the opposite direction. The numerical results (see (1.1)) suggest that three of the successive four couples $2^n - 3$ and $3^n - 2$ are relatively prime. Yet we do not know whether there are infinitely many exponents n for which the numbers $2^n - 3$ and $3^n - 2$ are relatively prime. The conjecture is that there are infinitely many such exponents.

References

[1] Banaszak, G., *Mod p logarithms* $\log_2 3$ *and* $\log_3 2$ *differ for infinitely many primes*, Ann. Math. Siles. **12** (1998), 141–148.

[2] Bart de Smit, and R. Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. **31** (1994), 213–215.

[3] Győry, K., *Some recent applications of $S-$unit equations*, Astérisque **209** (1992), 17–38.

[4] Pólya, G., und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Zweiter Band. Springer Verlag, 1964.

[5] Silverman, J. H., and J. Tate, *Rational points on elliptic curves*, Springer Verlag, 1992.

Address: Instytut Matematyki, Uniwersytet Śląski, Bankowa 14, 40-007 Katowice
E-mail: `szymicze@ux2.math.us.edu.pl`
Received: 27 Apr 2000