ON THE PRIME DIVISORS OF GCD$(3^n - 2, 2^n - 3)$

Anatoly S. Izotov
Dostoevsky str. 7, apt. 12, Novosibirsk, 630091, Russia
e-mail: izotov@nskes.ru

(Submitted August 2002-Final Revision February 2003)

In 1997 Schinzel asked for an argument to disprove that for sufficiently large prime q, the number $3^m - 2$ is divisible by q if and only if $2^m - 3$ is divisible by q. This was resolved by Banaszak [1]. Schinzel's question raises an interesting problem, posed by K. Szymiczek in [3], concerning $d_n = \gcd(3^n - 2, 2^n - 3)$. It is known that for all $n < 3000, d_n = 1$ if $n \equiv 0, 1, 2 \mod 4$, and $d_n = 5$ if $n \equiv 3 \mod 4$. But for $n = 3783, d_n = 26665$. In [5], by congruential techniques, the following statement was proved.

$$26665 | \gcd(3^n - 2, 2^n - 3) \text{if and only if } n \equiv 3783 \bmod 5332.$$

In this note we will give a condition for a prime $q > 3$ to divide d_m, using elementary properties of linear recurrences. Let $x_n = 3^n - 2$ and $y_n = 2^n - 3$ for $n \geq 0$. We shall prove

Theorem: Let $q > 3$ be a prime number. If $x_{n-1} \equiv 0 \mod q$ and $y_{n-1} \equiv 0 \mod q, n \geq 1$, then $u_n \equiv 0 \mod q$ and $6^{n-2} \equiv 1 \mod q$, where $\{u_n\}, n \geq 0$ is the recurrent sequence of order two $u_{n+2} = 5u_{n+1} - 6u_n,\ u_0 = 0, u_1 = 1$, that is, $u_n = 3^n - 2^n$.

On the other hand, if $u_n \equiv 0 \mod q$ and $6^{n-2} \equiv 1 \mod q$ then either $x_{n-1} \equiv 0 \mod q$ and $y_{n-1} \equiv 0 \mod q$ or $3^{n-1} + 2 \equiv 0 \mod q$ and $2^{n-1} + 3 \equiv 0 \mod q$.

Proof: Since $3x_{n-1} = 3^n - 6 \equiv 0 \mod q$ and $2y_{n-1} = 2^n - 6 \equiv 0 \mod q$ we have $3x_{n-1} - 2y_{n-1} = 3^n - 2^n \equiv 0 \mod q$. Since $3^n - 2^n = u_n,\ u_n \equiv 0 \mod q$. Furthermore, $x_{n-1} \equiv 0 \mod q$ implies $3^{n-1} \equiv 2 \mod q$ and $y_{n-1} \equiv 0 \mod q$ implies $2^{n-1} \equiv 3 \mod q$. Multiplying both part of these congruencies, we have $6^{n-1} \equiv 6 \mod q$ implies $6^{n-2} \equiv 1 \mod q$. The first part of the theorem is proved.

Conversely, $u_n = 3^n - 2^n \equiv 0 \mod q$. Write $3^n \equiv \alpha \mod q$ for some integer α. Then $2^n \equiv \alpha \mod q$ and we have $6^n \equiv \alpha^2 \mod q$. Since $6^{n-2} \equiv 1 \mod q$ we have $\alpha^2 \equiv 36 \mod q$ whence $\alpha \equiv \pm 6 \mod q$. If $\alpha \equiv 6 \mod q$ then $3^n \equiv 6 \mod q$ implies $3^{n-1} - 2 = x_{n-1} \equiv 0 \mod q$ and $2^n \equiv 6 \mod q$ implies $2^{n-1} - 3 = y_{n-1} \equiv 0 \mod q$. If $\alpha \equiv -6 \mod q$ then $3^n \equiv -6 \mod q$ implies $3^{n-1} + 2 \equiv 0 \mod q$ and $2^n \equiv -6 \mod q$ implies $2^{n-1} + 3 \equiv 0 \mod q$. The theorem is proved.

So, if $u_n \equiv 0 \mod q$ and $6^{n-2} \equiv 1 \mod q$ then q is a possible divisor of d_{n-1}. The table of factorizations of the numbers $u_n = 3^n - 2^n$ for many n is given in [4]. By the theory of linear recurrences of order two, for each prime number $q > 3$ there are infinitely many indexes m such that $u_m \equiv 0 \mod q$. If l is the least of them, then $n = xl$ for any integer x. Analogously, there exists a minimal integer k such that $6^k \equiv 1 \mod q$ and $n - 2 = yk$ for any integer y. Note, that $\gcd(l, k) = 1$ or 2, since $\gcd(n, n-2) = 1$ or 2. It is known that $q = al + 1, q = bk + 1$ for some integers $a, b \geq 1$. Let $\gcd(l, k) = 1$. We have $al = bk$ implies $a = \gamma k, b = \gamma l$ for any integer $\gamma > 1$. Therefore,

$$q = \gamma kl + 1. \tag{1}$$

If $\gcd(l, k) = 2$ and $l = 2l_1, k = 2k_1, \gcd(l_1, k_1) = 1$ then $q = 2al_1 + 1, q = 2bk_1 + 1$ for some integers $a, b \geq 1$. In this case

$$q = 2\gamma k_1 l_i + 1 \ \gamma \geq 1. \tag{2}$$

For some prime q, suppose there exist k and l which satisfy (1) or (2). To determine n we have the Diophantine equation

$$lx - ky = 2. \tag{3}$$

The method of solution this kind of equation is described, for example, in [2]. The least solution of (3) gives $n-1 = lx-1$ and d_{n-1} or $\gcd(3^{n-1}+2, 2^{n-1}+3)$ is divisible by q.

For known q such as $q = 5$ we have $l = 2, k = 1$. Equation (3), $2x - y = 2$ gives $x = 2$, $y = 2$ and $n - 1 = 3$. For $q = 5333$ we have $l = 86, k = 31$. Equation $86x - 31y = 2$ has the solution $x = 44, y = 122$ and $n - 1 = 3783$.

Since prime q has the form (1) or (2) then either k or l is less then $\sqrt{2q}$. Together with $\gcd(k, l) = 1$ or 2 it gives a fast algorithm for determining such q. In this algorithm for given prime q for $j = 1, 2, ..., [\sqrt{2q}]$ is calculated $A \equiv u_n \mod q$ and $B \equiv 6^n \mod q$. If $A = 0$ then $l = j$, if $B = 1$ then $k = j$. After then it is found m - the maximal divisor of $(q-1)/j$, such that $\gcd(m, j) = 1$.

Further we might compute only A or B up to m or $2m$. If $B = 1 (A = 0)$, then $k = j (l = j)$. Now we find $d = \gcd(k, l)$. If $d = 1$ or 2, then we solve (3), find $n - 1$ and direct compute $\alpha \equiv 2^{n-1} \mod q$, $\beta \equiv 3^{n-1} \mod q$. If $\alpha = 3$ and $\beta = 2$, then q is the divisor of d_{n-1}, else we give next prime q.

The search up to $2 \cdot 10^7$ gives, except for $q = 5$ and $q = 5333$, only one prime $q = 18414001$. In this case, $k = 99, l = 7750, \gcd(99, 7750) = 1$. The Diophantine equation $7750x - 99y = 2$ has minimal solution $x = 92, y = 7202$, hence $n - 1 = 712999$. Direct calculation gives $3^{712999} \equiv 2 \mod 18414001, 2^{712999} \equiv 3 \mod 18414001$, so $\gcd(3^{712999} - 2, 2^{712999} - 3) \geq 18414001$.

REFERENCES

[1] G. Banaszak. "Mod p Logarithms $\log_2 3$ and $\log_3 2$ Differ for Infinitely Many Primes." *Ann. Math. Siles* **12** (1998): 141-48.

[2] H. Davenport. *The Higher Arithmetic. An Introduction in the Theory of Numbers.* New York: Harper & Brothers, 1961.

[3] "Foreword. The 2nd Czech and Polish Conference on Number Theory." *Ann. Math. Siles* **12** (1998): 9-172.

[4] H. Riesel. "Prime Numbers and Computer Methods for Factorization." Boston: Birkhäuser Boston Inc, 1985.

[5] K. Szymiczek. "On the Common Factor of $2^n - 3$ and $3^n - 2$." *Funct. Approx. Comment. Math.* **28** (2000): 221-32.

AMS Classification Numbers: 11A41, 11B37

✠ ✠ ✠