L'Enseignement Mathématique, t. 46 (2000), p. 385–389

THE SIXTH FERMAT NUMBER AND PALINDROMIC CONTINUED FRACTIONS

by Freeman DYSON

ABSTRACT. An elementary argument is presented, verifying the known factorization of the sixth Fermat number $2^{64}+1$. The verification is made more elegant by using an old theorem of Serret concerning palindromic continued fractions.

It is easy to explain why the fifth Fermat number $2^{32}+1$ is divisible by 641 [Hardy and Wright, 1938]. The prime 641 has the two representations

$$641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4. \tag{1}$$

The congruence

$$2^{32} = 2^4 \cdot 2^{28} \equiv -5^4 \cdot 2^{28} = -(5 \cdot 2^7)^4 \equiv -1 \pmod{641} \tag{2}$$

follows immediately from (1).

The purpose of this note is to explain in a similarly elementary way why the sixth Fermat number $2^{64}+1$ is divisible by 274177. The divisor has the representation

$$q = 274177 = 1 + 2^8 f, \qquad f = (2^6 - 1)(2^4 + 1), \tag{3}$$

and it is easily verified that

$$2^{24} - 1 = fg, \qquad g = (2^6 + 1)(2^8 - 2^4 + 1). \tag{4}$$

We look for a factorization of the form

$$2^{64} + 1 = (x^2 + y^2)(z^2 + w^2), \qquad 2^{32} - i = (x + iy)(z - iw), \tag{5}$$

so that we require integers x, y, z, w satisfying

$$xz + yw = 2^{32}, \qquad xw - yz = 1, \qquad x^2 + y^2 = q. \tag{6}$$

When $z = gx$, $w = gy$, the right side of (5), $(x+iy)g(x-iy)$, becomes gq; and $gq = 2^{32} + a$, very close to 2^{32}, with the difference $a = g - 2^8 = 15409$