Problem for 2000 September

communicated by Dan Jurca

The following problems are taken from the delightful *Conjecture and Proof* by Miklós Laczkovich. The first concerns the Fermat numbers F_n, and the second concerns the numbers F_n+2.

The Fermat number F_n is $2^{2n}+1$ where n is a non-negative integer. Thus

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65{,}537$$

It is easy to show that F_0, F_1, F_2, F_3, and F_4 are primes, and Pierre Fermat conjectured around 1640 that each F_n is prime. However, in 1732 Euler found that 641 divides F_5; in fact $F_5=4{,}294{,}967{,}297=641\times 6{,}700{,}417$; in 1880 it was found that 274,177 divides F_6; and in 1970 it was found that F_7 is the product of two primes consisting of 17 and 22 decimal digits, respectively. It is now known that F_n is composite if $5 \le n \le 24$; no Fermat prime is known beyond F_4. Gauss showed that the regular n-gon is constructible with unmarked straightedge and compass if and only if n equals a power of 2 times a product of distinct Fermat primes.

1. Show that if $2 \le n$, then $F_n \equiv 7 \pmod{10}$; *i.e.*, show that if $2 \le n$, then when F_n is written in base 10 the last digit is a 7.

2. Write $G_n=F_n+2$, so that $G_n=2^{2n}+3$. Show that there exist infinitely many n such that G_n is composite.

Solution by Dan Jurca

Each assertion can be proved by mathematical induction.

1.

First we observe

$$\begin{aligned} 1 \le n \Rightarrow F_n &= 2^{2^n}+1 \\ &= 2^{2^{n-1}\times 2}+1 \\ &= (2^{2^{n-1}})^2+1 \\ &= (F_{n-1}-1)^2+1 \\ &= F_{n-1}{}^2-2F_{n-1}+2. \end{aligned}$$

Now $F_2=17$; if $3 \le n$ and $F_{n-1} \equiv 7 \pmod{10}$, then there exists some integer q such that $F_{n-1}=10q+7$, and then

$$\begin{aligned} F_n &= F_{n-1}{}^2-2F_{n-1}+2 \\ &= (10q+7)^2-2(10q+7)+2 \\ &= 100q^2+140q+49-20q-14+2 \\ &= 100q^2+120q+37 \\ &= 10(10q^2+12q+3)+7, \end{aligned}$$

so that $F_n \equiv 7 \pmod{10}$ as well. Hence by induction on n: $2 \le n \Rightarrow F_n \equiv 7 \pmod{10}$.

2.

We shall show that $0 \le k \Rightarrow 7 | G_{2k+3}$.
This is immediate if k=0, since $G_3=2^{2^3}+3=2^8+3=256+3=259=7\times 37$.
Next we observe

$$\begin{aligned} 1 \le n \Rightarrow G_n &= 2^{2^n}+3 \\ &= 2^{2^{n-1}\times 2}+3 \\ &= (2^{2^{n-1}})^2+3 \\ &= (G_{n-1}-3)^2+3 \\ &= G_{n-1}{}^2-6G_{n-1}+12, \quad \text{so that} \\ 2 \le n \Rightarrow G_n &= (G_{n-2}{}^2-6G_{n-2}+12)^2-6(G_{n-2}{}^2-6G_{n-2}+12)+12 \\ &= G_{n-2}{}^4-12G_{n-2}{}^3+54G_{n-2}{}^2+222G_{n-2}+84 \end{aligned}$$

$$=(G_{n-2}{}^3-12G_{n-2}{}^2+54G_{n-2}+222)G_{n-2}+84.$$

Then since $7|84$, we have $2 \le n$ and $7|\ G_{n-2} \Rightarrow 7|G_n$. Thus by induction on k we have $0 \le k \Rightarrow 7|G_{2k+3}$, as asserted.

Therefore G_n is composite-indeed, divisible by 7-for infinitely many n.