BEGINNERS' CORNER

EDITED BY DMITRI THORO, SAN JOSE STATE COLLEGE

DIVISIBILITY II

We shall continue our investigation of some "background material" for the beginning Fibonacci explorer. Whenever necessary, we may assume that the integers involved are not negative (or zero).

1. DEFINITIONS

Two integers a and b are relatively prime if their greatest common divisor (g. c. d.) is 1. When convenient we will use the customary abbreviation (a, b) to designate the g. c. d. of a and b. Finally, as previously implied, we shall say that n is composite if n has more than two divisors.

2. ILLUSTRATIONS

E1. If $d \mid a$ and $d \mid b$, then $d \mid (a \pm b)$; i. e., a common divisor of two numbers is a divisor of their sum or difference.

PROOF: $d \mid a$ means there exists an integer a such that $a = a'd$. Similarly, we may write $b = b'd$. Thus $a \pm b = d(a' \pm b')$ which proves that $d \mid (a \pm b)$. [This follows from the definition of divisibility.]

E2. If $d = (a, b)$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$; i. e., if two numbers are divided by their g. c. d., then the quotients are relatively prime. [This result is a widely used "tool."]

PROOF: Since d is the g. c. d. of a and b, $\frac{a}{d}$ and $\frac{b}{d}$ are certainly integers; let us call them a' and b', respectively. Thus $a = a'd$, $b = b'd$, and we are to show that $(a', b') = 1$. The trick is to use an indirect argument.

Suppose $(a', b') = d' > 1$. Then (there exist integers a'' and b'' such that) $a' = a''d'$ and $b' = b''d'$. This implies $a = a'd = a''d'd$ and $b = b'd = b''d'd$; i. e., $d'd$ is a common divisor of a and b. But we assumed $d' \neq 1$, which means $dd' > d$ – contrary to the fact that d is the greatest common divisor of a and b.

E3. If a and b are relatively prime, what can you say about the g. c. d. of $a + b$ and $a - b$? For example, $(13 + 8, 13 - 8) = 1$, but $(5 - 3, 5 - 3) = 2$. It turns out, however, that these are the only possibilities!

If $(a,b) = 1$, then $(a + b, a - b) = 1$ or 2.

PROOF: Let $(a + b, a - b) = d$. Then by E1, $d \mid [(a + b) \pm (a - b)]$; i.e., $d \mid 2a$ and $d \mid 2b$.

(i) If d is even, set $d = 2K$. Then from $2a = 2Ka'$, $2b = 2Kb'$ we have $a = Ka'$, $b = Kb'$. Therefore K must be 1 (why?), and hence $d = 2$.

(ii) Similarly if d is odd, then d would have to divide both a and b, whence $d = 1$.

Can you see what objection a pedantic reader might have to this proof?

E4. The following is a special case of a result due to Sophie Germain, a French mathematician (1776–1831).

$$n^4 + 4 \text{ is composite for } n > 1 .$$

PROOF: Unlike the preceding illustrations, here one needs to stumble onto a factorization. $n^4 + 4 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$ does the trick, for this shows that $N = n^4 + 4$ is divisible by a number between 1 and N and hence must be composite.

E5. We now consider one of the simplest properties of Fibonacci numbers.

Two consecutive Fibonacci numbers are always relatively prime.

PROOF: Certainly this is obvious for the first few numbers: 1, 1, 2, 3, 5, 8, ... Let us use an indirect argument. Suppose F_n and F_{n+1} is the first pair for which $(F_n, F_{n+1}) = d > 1$. Now examine the pair F_{n-1} and F_n. Since $F_{n+1} - F_n = F_{n-1}$, d is a divisor of F_{n-1} (for $d \mid F_{n+1}$, $d \mid F_n$ and hence, by E1, their difference). This means that F_{n-1} and F_n are not relatively prime – a contradiction to our assumption that F_n and F_{n+1} is the first such pair.

3. SOME USEFUL THEOREMS

T1. Any composite integer n has at least one prime factor.

PROOF: (i) Since n is composite, it must have at least one divisor greater than 1 and less than n.

(ii) Let d be the smallest divisor of n such that $1 < d < n$.

(iii) Suppose d is composite; let $d' \mid d$, $1 < d' < d$.

(iv) Thus we have $n = n_1 d = n_1 d' d''$; i.e., $d' \mid n$ but $d < d'$ — a contradiction to the definition of d. Therefore d must be a prime.

T2. Given $n > 1$. Suppose that the quotient q, in the division of n by a, is less than a. If n is not divisible by 2, 3, 4, . . . , $(a - 1)$, a, then n is a prime.

PROOF: (i) If q (q < a) is the quotient and r the remainder in the division of n by a, we may write

$$\frac{n}{a} = q + \frac{r}{a}, \quad 0 \leq r < a .$$

(ii) Assume that n is not divisible by 2, 3, $\cdots$, a but has a divisor d, $1 < d < n$. We shall show that this leads to a contradiction.

(iii) Since $d|n$, $n = dd'$, where $1 < d' < n$.

(iv) By (ii), $d' > a$ and by (i) $a > q$; hence $d' > q$ or $d' \geq q + 1$. Also $d > a$; multiplying $d' \geq q + 1$ by $d > a$, we arrive at

(v) $n = dd' > aq + a$. But by (i), $n = aq + r < aq + a$ since $r < a$. This is the desired contradiction which proves that n cannot be divisible by d, $1 < d < n$, and hence must be a prime.

T3. If $n > 1$ is not divisible by $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \cdots, p_k$, where p_k is the largest prime whose square does not exceed n, then n is a prime.

PROOF: Assume $a^2 \leq n < (a + 1)^2$ and that n is not divisible by 2, 3, $\cdots$, (a - 1), a. Then $n = dd'$ implies $d \geq a + 1$, $d' \geq a + 1$, whence $n = dd' \geq (a+1)^2$ — a contradiction. Thus n must be prime. The reader should convince himself that here (as well as in T2) it suffices to consider only prime divisors $\leq \sqrt{n}$.

4. PROBLEMS

1.1 Suppose that

(i) p is the smallest prime factor of n and

(ii) $p > \sqrt[3]{n}$.

What interesting conclusion can you draw?

1.2 Prove that two consecutive Fibonacci numbers are relatively prime by using one of the identities on p. 66 (Fibonacci Quarterly, February, 1963).

1.3 Prove that if p and p + 2 are (twin) primes, then p + 1 is divisible by 6. (Assume $p > 3$.) [This problem was suggested by James Smart.]

1.4 Prove that if n is divisible by k, $1 < k < n$, then $2^n - 1$ is divisible by $2^k - 1$. For example, $2^{35} - 1 = 34\ 359\ 738\ 367$ is divisible by $2^5 - 1 = 31$ and $2^7 - 1 = 127$.

1.5 Prove that there are infinitely many primes. Hint: Assuming that p_n is the largest prime, Euclid considered the expression $N = 1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n$. Now either N is prime or N is composite. Complete his proof by investigating the consequences of each alternative.

Additional hints may be found on p. 80.

FIBONACCI FORMULAS

Maxey Brooke, Sweeny, Texas

If you have a favorite Fibonacci formula, send it to us and we will try to publish it. Some historically interesting ones are shown below.

1. Perhaps the first Fibonacci formula was developed by Simpson in 1753.

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

2. A very important formula was developed in 1879 by an obscure French mathematician, Aurifeuille. In fact, it is his one claim to fame.

$$L_{5n} = L_n(L_{2n} - 5F_n + 3)(L_{2n} + 5F_n + 3)$$

3. The only formula involving cubes of Fibonacci numbers given in Dickson's "History of the Theory of Numbers" is due to Lucas.

$$F_{n+1}^3 + F_n^3 - F_{n-1}^3 = F_{3n}$$

The late Jekuthiel Ginsburg offers $F_{n+2}^3 - 3F_n^3 + F_{n-1}^3 = 3F_{3n}$.

4. The recursion formula for sub-factorials is similar to the one for Fibonacci numbers: $P_{n+1} = n(P_n + P_{n-1})$; $P_0 = 1$, $P_1 = 0$.

5. Fibonacci numbers have been related to almost every other kind of number. Here is H. S. Vandiver's relation with Bernoulli numbers.

$$\sum_{k=0}^{\overline{p-3}} B_{2k}F_{2k} \equiv \frac{1}{2} \pmod p \quad \text{if } p = 5a \pm 1$$

$$\sum_{k=0}^{\overline{p-3}} B_{2k}F_{2(k-1)} \equiv 1 \pmod p \quad \text{if } p = 5a \pm 2$$

$\overline{p-3}$ denotes the greatest integer not exceeding $(p-3)/2$.

I think that this is a good idea.

Ed.