Class Tutorial - Divisibility and Primality

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Tuesday 8th November 2011

Questions - Divisibility I

1. Let us define the height $h(a)$ of an integer $a \geqslant 2$ to be the greatest n such that Euclid's algorithm requires n steps to compute $gcd(a, b)$ for some positive $b < a$ (that is, $gcd(a, b) = r_{n-1}$). Show that $h(a) = 1$ if and only if $a = 2$, and find $h(a)$ for all $a \leqslant 8$.
2. The Fibonacci numbers $f_n = 1, 1, 2, 3, 5, \ldots$ are defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for all $n \geqslant 1$. Show that $0 \leqslant f_n < f_{n+1}$ for all $n \geqslant 2$. What happens if Euclid's algorithm is applied when a and b are a pair of consecutive Fibonacci numbers f_{n+2} and f_{n+1}? Show that $h(f_{n+2}) \geqslant n$.

Questions - Divisibility II

3. Suppose that $a > b > 0$, that Euclid's algorithm computes $gcd(a, b)$ in n steps, and that a is the smallest integer with this property (that is, if $a' > b' > 0$ and $gcd(a', b')$ requires n steps, then $a' \geqslant a$); show that a and b are consecutive Fibonacci numbers $a = f_{n+2}$ and $b = f_{n+1}$ (Lamé's Theorem, 1845).
4. Show that $h(f_{n+2}) = n$, and f_{n+2} is the smallest integer of this height.

Questions - Divisibility III

5. Show that $f_n = (\phi^n - \psi^n)/\sqrt{5}$. where ϕ, ψ are the positive and negative roots of $\lambda^2 = \lambda + 1$. Deduce that $f_n = \{\phi^n/\sqrt{5}\}$, where $\{x\}$ denotes the lowest integer closest to x. Hence obtain the approximate upper bound

   $$\log_\phi(a\sqrt{5}) - 2 = \log_\phi(a) + \frac{1}{2}\log_\phi(5) - 2 \approx 4.785\log_{10}(a) - 0.328$$

   for the number of steps required to compute $gcd(a, b)$ by Euclid's algorithm, where $a \geqslant b > 0$.

6. Show that if a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that $a = qb + r$ and $-|b|/2 < r < |b|/2$. Use this result to devise an alternative algorithm to Euclid's for calculating greatest common divisors (the least remainders algorithm).

Questions - Divisibility IV

7. Use the least remainders algorithm to compute $gcd(1066, 1492)$ and $gcd(1485, 1745)$, and compare the numbers of steps required by this algorithm with those required by Euclid's algorithm.
8. What happens if the least remainders algorithm is applied to a pair of consecutive Fibonacci numbers?
9. Show that if a and b are coprime positive integers, then every integer $c \geqslant ab$ has the form $ax + by$ where x and y are non-negative integers. Show that the integer $ab - a - b$ does not have this form.

University of Bedfordshire

Questions - Primality

1. For which prime p is $p^2 + 2$ also prime?
2. Show that if $p > 1$ and p divides $(p-1)! + 1$, then p is prime.
3. Extend the theorem of prime-power factorisation so that it describes the factorisation of all positive rational numbers.
4. Show that if $n, q \geqslant 1$ then the number of multiples of q among $1, 2, \ldots, n$ is $\lfloor n/q \rfloor$. Hence show that if p is prime and $p^e || n!$, then $e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots$
5. What is the relationship between the number of 0s at the end of the decimal expansion of an integer n, and the prime-power factorisation of n? Find the corresponding result for the base b expansions of n (where we write $n = \sum_{i=0}^{k} a_i b^i$ with $0 \leqslant a_i < b$).
6. Show that $F_0 F_1 \ldots F_{n-1} = F_n - 2$ for all $n \geqslant 1$.
7. Evaluate the Mersenne number M_{17}, and determine whether it is prime.