cwork2b.tex 15/10/2003

MAS/202 Algorithmic Mathematics: Coursework 2

Franco Vivaldi

DEADLINE: Wednesday of week 4, at 12:00 pm.

CONTENT: Primes.

[$\not{e}$, n] : no mathematical symbols are allowed; use approximately n words.

MicroESSAY : Write an essay on prime numbers. [$\not{e}$, 100]

Problem 1.

(*a*) Let a, b, c, x, y be integers, such that a divides b and a divides c. Show that a divides $xb + yc$.

(*b*) Show that, if n is odd, then $(n^2 \,\mathrm{MOD}\, 8) = 1$.
[*Hint:* remember that $a \,\mathrm{MOD}\, b = r$ means $a = qb + r$, for some q. How do you represent an odd integer?]

(*c*) Using the above, show that $x^2 + y^2 = z^2$ cannot be true in integers, when both x and y are odd. Give an example.
[*Hint:* treat the case z even and odd separately.]

Problem 2. Let A, X be sets, with $A \subset X$, and let $\mathcal{C}_A$ be the characteristic function of A in X. Consider the following algorithm

```
Algorithm CA
INPUT x ∈ X
OUTPUT C_A(x)
return ??;
end;
```

White the `return` statement corresponding to the case $X = \mathbb{Z}$ and A the set of

(*i*) the divisors of $2^{100} - 1$.

(*ii*) the even multiples of 7.

(*iii*) the integers divisible by 3 or 7, but not by both.

(*iv*) the positive primes with at least 10 decimal digits.

(*v*) the positive odd primes p such that $2p + 1$ is also prime.

(*vi*) the primes which differ from their nearest multiple of 100 by a prime.

Use MOD for divisibility and `IsPrime` for primality testing. Try to make boolean expressions efficient. Assume they are evaluated from left to right (unless there are parentheses), and that redundant evaluations are not performed (e.g., if x is FALSE, the value of x AND y is known without evaluating y).

Problem 3. Use `IsPrime` to decide the primality of 437.

Problem 4. Use `IntegerFactorization` to determine the prime factorization of 3626.
[This is a 2001 final examination question. Check your result by multiplying out the factors.]

Problem 5. Consider the following algorithm

`Algorithm IntSqrt`
`INPUT`: $x \in \mathbb{Z}$, $x \geq 0$.
`OUTPUT`: the largest integer not exceeding $\sqrt{x}$.

(*a*) Write it, performing only integer arithmetic. (You need a loop.)

(*b*) Explain how it works. [$\not\in$, 50]