21-320 Homework Set 7

James Cummings

April 11, 2000

Due Mon 17 April. I encourage submission by email (preferably as a PostScript file) to `maplehw@asdb.math.cmu.edu`.

1. A celebrated theorem in number theory (the Prime Number Theorem, proved by Chebyshev) states that there are roughly $\frac{n}{\ln(n)}$ primes less than n.

   (a) Use the Prime Number Theorem to predict the number of primes p such that $10^6 < p < 10^6 + 10^5$.

   (b) Compute the exact number of such primes and compare your answer with the approximate one.

2. Recall that $\phi(N)$ is the number of integers a such that $0 < a < N$ and $\gcd(a, N) = 1$. Recall also that if N is the product of distinct primes p and q then $\phi(N) = (p-1)(q-1)$.

   I tell you that N is a product of two distinct primes, and also that N equals

   ```
   71230886527397475528902959842062683921344888484583255939615\
   11926098127930826919074574335127781473351746240614365711OO\
   34449238599477010735686218053250465233763709668294651792 46\
   38185417865741849422076653448639649550966763391190180315 68\
   2002829226033237
   ```

   and $\phi(N)$ equals

```
7123088652739747552890295984206268392134488848458325593961 5\
```

Factorise N.

3. My public RSA key is (N, e) where N is the integer from the previous question and e equals

```
587826329714726097359772478548136792078300110365740286242 63\
```

Decode the message

which was encrypted using the key (N, e).

(I coded this using the convention 0=blank, 1=A,2=B etc from class)

4. A positive integer $n > 1$ is called a *Carmichael number* if and only if it satisfies all of the following conditions:

   (a) n is not prime.

   (b) For all integers b with $0 < b < n$, if $gcd(b, n) = 1$ then b^{n-1} is congruent to 1 modulo n.

   Find as many Carmichael numbers as you can. Encouraging hint: there is at least one Carmichael number less than one thousand.

5. It's a nice fact from number theory that if a and b are non-zero integers and $d = gcd(a, b)$ then there are integers m and n such that $d = ma+nb$. For example the gcd of 8 and 14 is 2, and $2 = 3 \times 14 - 5 \times 8$.

   Write a program which takes a and b as arguments and returns a suitable pair m, n.