The University of Sydney
School of Mathematics and Statistics

Computer Tutorial 10 (Week 11)

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

There is no special data file to be loaded this week.

1. The MAGMA function `PrimesUpTo` returns the set of prime numbers up to a specified number. So `PrimesUpTo(1000);` returns the set of primes less than 1000. Try it, and then use commands such as `#PrimesUpTo(1000);` to find the number of primes less than 1000, 2000, ..., 10000.

2. Let $\pi(N)$ be the number of primes less than or equal to the positive integer N. The famous Prime Number Theorem (whose proof is beyond this course) states that $\pi(N) \sim \frac{N}{\ln(N)}$ as $N \to \infty$. That is, $\pi(N)\ln(N)/N \to 1$ as $N \to \infty$, though the convergence is relatively slow. Compute $\pi(N)\ln(N)/N$ for $N = 10^i$, for each i from 1 to 8. (Remember that the MAGMA function `Log` computes natural logarithms.)

3. As seen in lectures, the best primes p to use in the Elgamal cryptosystem are those for which $\frac{p-1}{2}$ is also prime; these are called *safe* primes. Define the following function which returns the set of safe primes up to a specified number:

```
safeprimes:= function(N)
  SP:={}; p:=3;
  while p le N do
    if IsPrime((p-1) div 2) then
      Include(~SP,p);
    end if;
    p:=NextPrime(p);
  end while;
  return SP;
end function;
```

Then use it to find all the safe primes less than 1000, and the number of safe primes less than 1000, 2000, ..., 10000.

4. You can interpret the Prime Number Theorem as saying then the probability that a random number less than N is prime is about $1/\ln(N)$, for N large enough. If the events that N is prime and that $\frac{N-1}{2}$ is prime were independent (which they are not), the probability of them both occurring simultaneously would be the product of their separate probabilities, about $(1/\ln(N))(1/\ln(N/2))$. So the number of safe primes less than N would be about $N(1/\ln(N))(1/\ln(N/2))$. Compute this for $N = 1000, 2000, \ldots, 10000$, and compare with the actual numbers you found in the previous exercise.

5. A more sophisticated argument suggests that a better estimate for the number of safe primes less than N would be $CN/(\ln(N/2))^2$, where C is the *twin prime constant* defined

to be $\prod_{p\geq 3} \frac{p(p-2)}{(p-1)^2}$, the product being over all odd prime numbers. Use MAGMA to find an approximation to C:

```
C:=RealField()!(&*[p*(p-2)/(p-1)^2 : p in PrimesUpTo(10000) | p gt 2 ]);
```

and test this new estimate against the actual numbers found in Exercise 3.

6. Put $N = 10^{300}$, and assume that $CN/(\ln(N/2))^2$ approximates the number of safe primes less than N. So the probability that a randomly chosen number less than N is a safe prime is $t = C/(\ln(N/2))^2$. Now imagine choosing k random numbers less than N, in the hope that one of them is a safe prime. How large does k have to be to make the probability of success greater than 0.5? (Hint: the probability of success is $1-(1-t)^k$.)

7. In MAGMA's terminology, if `p` is a prime then `FiniteField(p)` is the set `{0,1,...,p-1}`, with addition and multiplication defined to be the same as ordinary addition and multiplication followed by reduction modulo `p`. MAGMA's "coercion operator" `!` can be used to convert an integer to an element of `FiniteField(p)`, or vice versa. Type `F:=FiniteField(97);` and define `a:=F!50; b:=F!77;`. Check that `a*b` and `a+b` agree with what you expect. Similarly, check that `a^111;` agrees with `Modexp(50,111,97);` and that `b^(-1);` agrees with `InverseMod(77,97);`.

8. We now want to do some calculations with polynomials modulo 97. Type or copy

```
P<x>:=PolynomialRing(F);
f5:=(x-1)*(x-2)*(x-3)*(x-4)/((5-1)*(5-2)*(5-3)*(5-4));
f4:=(x-1)*(x-2)*(x-3)*(x-5)/((4-1)*(4-2)*(4-3)*(4-5));
f3:=(x-1)*(x-2)*(x-4)*(x-5)/((3-1)*(3-2)*(3-4)*(3-5));
f2:=(x-1)*(x-3)*(x-4)*(x-5)/((2-1)*(2-3)*(2-4)*(2-5));
f1:=(x-2)*(x-3)*(x-4)*(x-5)/((1-2)*(1-3)*(1-4)*(1-5));
```

Observe that the polynomial `f5` should take the value 0 when `x` is 1 or 2 or 3 or 4, and 1 when `x` is 5, and similarly for `f4` etc. You can check this all at once with

```
[ [ Evaluate(fi,xj) : xj in [1..5] ] : fi in [f1,f2,f3,f4,f5] ];
```

Now define `a1:=73; a2:=50; a3:=36; a4:=82; a5:=17;` and

```
f:=a1*f1+a2*f2+a3*f3+a4*f4+a5*f5;
```

What values will `f` take at 1, 2, 3, 4 and 5? Check it.

9. Suppose `S` is a top-secret number about which five people P_1, P_2, P_3 P_4 and P_5 have been given partial information. Specifically, they have been told that `S` is less than the prime `p`, which is 447555834974539, and that `S` is the constant term $f(0)$ of a quadratic polynomial $f(x)$ over `FiniteField(p)`. In addition, person P_i was told the value of $f(i)$. Unfortunately, P_2 and P_5 have disappeared, so P_1, P_3 and P_4 hold an urgent meeting to share their information. Given that $f(1) = 196231291191342$, $f(3) = 195412581909834$, and $f(4) = 163633523397347$, find `S`.