Congruences and All That

The goal of this handout is to show you how to solve congruences of the form $ax \bmod n = 1$. You can use this to compute the private key during the initialization of an RSA cryptosystem.

Solving $ax \bmod n = 1$ when $\gcd(a, n) = 1$.

Use Euclid's extended GCD algorithm to compute x: The algorithm, in Pascal, is:

```
begin        (* compute x such that ax mod n = 1, where 0 < a < n *)
      g[0] := n; g[1]:= a; u[0] := 1; v[0] := 0; u[1] := 0; v[1] := 1; i := 1;
      while g[i] <> 0 do begin (* loop invariant: g[i] = u[i] * n + v[i] * a *)
            y[i] := g[i-1] div g[i];
            g[i+1] := g[i-1] - y[i] * g[i];
            u[i+1] := u[i-1] - y[i] * u[i];
            v[i+1] := v[i-1] - y[i] * v[i];
            i := i + 1;
      end;
      x := v[i-1];
      if x < 0 then
            x := x + n;
end.
```

For example, to solve $3x \bmod 7 = 1$, calculate as follows:

i	g[i]	u[i]	v[i]	y	u[i] * n + v[i] * a
0	7	1	0		1 * 7 + 0 * 3 = 7
1	3	0	1	2	0 * 7 + 1 * 3 = 3
2	1	1	-2	3	1 * 7 + (-2) * 3 = 1
3	0				(-3) * 7 + 7 * 3 = 0

Hence, $x = -2 + 7 = 5$.

First Congruence

In the first example of an RSA cipher, we chose $p = 5$ and $q = 7$. This means $n = pq = 35$, and $\phi(n) = (5–1)(7–1) = 24$. We must find d and e such that $de \bmod \phi(n) = 1$. We chose $d = 11$ and need to determine e. As $\gcd(11, 24) = 1$, we can use the above algorithm to solve $11e \bmod 24 = 1$:

i	g[i]	u[i]	v[i]	y	u[i] * n + v[i] * a
0	24	1	0		1 * 24 + 0 * 11 = 24
1	11	0	1	2	0 * 24 + 1 * 11 = 11
2	2	1	-2	5	1 * 24 + (-2) * 11 = 2
3	1	-5	11	2	(-5) * 24 + 11 * 11 = 1
4	0				

Hence, $e = 11$.

Second Congruence

In the second example, we chose $p = 53$ and $q = 61$. This means $n = pq = 3233$, and $\phi(n) = (53–1)(61–1) = 3120$. We must find d and e such that $de \bmod \phi(n) = 1$. We chose $d = 791$ and need to determine e. As $\gcd(791, 3120) = 1$, we can use the above algorithm to solve $791e \bmod 3120 = 1$

i	g[i]	u[i]	v[i]	y	u[i] * n + v[i] * a
0	3120	1	0		1 * 3120 + 0 * 791 = 3120
1	791	0	1	3	0 * 3120 + 1 * 791 = 791
2	747	1	-3	1	1 * 3120 + (-3) * 791 = 747
3	44	-1	4	16	(-1) * 3120 + 4 * 791 = 44
4	43	17	-67	1	17 * 3120 + (-67) * 791 = 43
5	1	-18	71	43	(-18) * 3120 + (71) * 791 = 1
6	0				

Hence, $e = 71$.

Acknowledgement: This algorithmis from Figure 1.21 in *Cryptography and Data Security*, by Dorothy Denning, published by the Addison-Wesley Publishing Co., Reading, MA, and ©1984.