Crypto HW #5 -- Primality Tests and Factoring Algorithms

1) Please use the continued fraction attack on the RSA public key (n, e) = (66511, 43995) to factor n and find the associated private key (n, d).

2) Please give (sufficient) conditions for a continued fraction attack on an RSA public key to be assured success, and create an RSA public key that avoids these conditions.

3) Please check the numbers n = 51, 91 and 671 for primality using the Miller-Rabin test with a=3, and use Fermat factorization to give a non-trivial factorization when possible.

4) For which of these n does the Fermat primality test show that n is composite?

5) How are the Fermat and Miller-Rabin primality tests related?

6) Please use the Pollard p-1 factoring algorithm with a = 2 and B <= 6 to attempt to factor n = 2573.

7) Under what assumptions on n is the Pollard p-1 factoring algorithm guaranteed to produce a non-trivial factorization of n? (**Challenge**: Can we use the Pollard p-1 method to factor 221 with a = 2? Please carefully explain your answer.)

8) Please use the quadratic sieve/Fermat factorization to factor n = 5917.

9) Please use the quadratic sieve to find a non-trivial factorization of n = 13703 based on the following factorizations of x^2 mod n, where 118 <= x <= 148.

```
sage: n = 13703
sage: factor(118^2 % n)
13 * 17
sage: factor(119^2 % n)
2 * 229
sage: factor(120^2 % n)
17 * 41
sage: factor(121^2 % n)
2 * 7 * 67
sage: factor(122^2 % n)
1181
sage: factor(123^2 % n)
2 * 23 * 31
sage: factor(124^2 % n)
7 * 239
sage: factor(125^2 % n)
2 * 31^2
sage: factor(126^2 % n)
41 * 53
```

```
sage: factor(127^2 % n)
2 * 1213
sage: factor(128^2 % n)
7 * 383
sage: factor(129^2 % n)
2 * 13 * 113
sage: factor(130^2 % n)
23 * 139
sage: factor(131^2 % n)
2 * 7 * 13 * 19
sage: factor(132^2 % n)
61^2
sage: factor(133^2 % n)
2 * 1993
sage: factor(134^2 % n)
4253
sage: factor(135^2 % n)
2 * 7 * 17 * 19
sage: factor(136^2 % n)
4793
sage: factor(137^2 % n)
2 * 17 * 149
sage: factor(138^2 % n)
7^2 * 109
sage: factor(139^2 % n)
2 * 53^2
sage: factor(140^2 % n)
5897
sage: factor(141^2 % n)
2 * 3089
sage: factor(142^2 % n)
7 * 13 * 71
sage: factor(143^2 % n)
2 * 3373
sage: factor(144^2 % n)
13 * 541
sage: factor(145^2 % n)
2 * 7 * 523
sage: factor(146^2 % n)
23 * 331
sage: factor(147^2 % n)
2 * 59 * 67
sage: factor(148^2 % n)
59 * 139
```