Mathematics 360 **Homework (due Oct 30)** A. Hulpke

Note: Starting with this set of homework problems, calculations such as $a^n \bmod p$ and $\mathrm{OrderMod}_p(a)$ become basic operations. I assume that you have a computer available to perform these effectively as a single operation as otherwise some problems become very work intensive if only using a basic calculator. (I am fully aware that you won't have a computer available in the exams and will limit the scope of exam problems accordingly.

41) In a Diffie-Hellman Key exchange you have agreed on prime $p = 10000000000000000039 = 10^{20} + 39$ and primitive root $g = 3$. Alice has sent you the number 5347 and you have chosen the random number 987654321. What number should you send to Alice? What is your shared secret key?

42) Use Shanks' Babystep-Giantstep algorithm to determine the discrete logarithm of 19 to base 2 modulo 1117. What interval length should you set?

43) (Follow-up on problem 36, "subgroups of cyclic groups")
a) Let p be a prime and $1 \le a < p$ with $k = \mathrm{OrderMod}_p(a)$. We want to show that any element of order dividing k must be a power of a, That is, show that if $1 \le b < p$ such that $\mathrm{OrderMod}_p(b) = m \mid k$, then there exists e such that $b \equiv a^e \pmod p$. (**Hint:** How many numbers $1 \le b < p$ have $\mathrm{OrderMod}_p(b) = m$? How many powers of a have $\mathrm{OrderMod}_p(a^x) = m$?)
b) Let g be a primitive root modulo p and $1 \le a < p$ such that $k = \mathrm{OrderMod}_p(a) < p - 1$. Let $h = g^{\frac{p-1}{k}}$. Show that a must be a power of h, and that this discrete logarithm calculation is easier that the one for base g.

44) Repeating the calculation of problem 42, i.e. $p = 1117$, $g = 2$, determine first $k = \mathrm{OrderMod}_p(19)$ and calculate $h = g^{\frac{p-1}{k}}$. Then, using the Babystep-Giantstep algorithm (with $\sqrt{\mathrm{OrderMod}_p(h)}$ steps!) write 19 as a power of h. Use this to determine the discrete logarithm of 19 to base 2 modulo p. Compare the result with the one from problem 42!

45) (The idea of the Pohlig-Hellman algorithm in an example)
We look again at the same task as in problem 42, but observe that $p - 1 = 31 \cdot 36$ with $\gcd(31, 36) = 1$.
a) We observe that $\mathrm{OrderMod}_p(19) = 372 = 12 \cdot 31$. Let $c = 40 \equiv 19^{12} \pmod p$ and $d = 203 \equiv 19^{31} \pmod p$. What is $\mathrm{OrderMod}_p(c)$ and $\mathrm{OrderMod}_p(d)$? Find e, f such that $19 = c^e \cdot d^f$.
b) Now let $r = 331 \equiv 2^{36} \pmod p$. Then (problems 19 and 41) we know that there must be an exponent m, such (with $c = 40 \equiv 19^{12} \pmod p$) that $r \equiv c^m \pmod p$.
Find this m, using the Babystep-Giantstep algorithm. (Note that we only need to search through intervals of length $\sqrt{\mathrm{OrderMod}_p(c)}$.
c) In the same way, setting $s = 883 \equiv 2^{31} \pmod p$, find n such that $s \equiv d^n \pmod p$ (with $d = 203 \equiv 19^{31} \pmod p$).

d) Using the values for e, f, m, n from parts a),b),c), determine the discrete logarithm of 19 to base 2 modulo p.
e) Count the number of arithmetic operations that were required. Compare with the number of operations required for problems 42 and 44).

46) Alice claims that she can read Bob's mind, namely that she can predict which choice Bob will make from the numbers 0 and 1. Bob is skeptical and they want to test this claim.
Clearly, Alice cannot tell her prediction, as Bob might then deliberately choose differently. Nor can Alice disclose her prediction only after Bob stated his choice, as he would be suspicious that she would claim to have predicted his choice. (We also assume that there is no impartial referee available to hold Alice's prediction *in escrow*, keeping it secret until Bob discloses his choice.)
They therefore set up the following scheme: They agree on a large prime p such that $p \equiv 3 \pmod 4$ and a primitive root a modulo p. Alice chooses a number x, such that the *second lowest* bit (i.e. the coefficient of 2 in a binary expansion) is the value she predicts, and tells Bob the result $a^x \bmod p$. (We assume that p is large enough so that Bob cannot solve the discrete logarithm problem.) Once Bob discloses his choice, Alice discloses x.
a) How would Bob check whether Alice's prediction was indeed correct. Why can both parties be sure that the other party did not cheat?
b) Why did Alice not choose the *lowest* bit (i.e. the even/odd bit) to indicate her prediction? And (this is fundamentally the same reason) why do they need to choose $p \equiv 3 \pmod 4$? (I.e. how could Bob deduce Alice's prediction if $p-1$ was a multiple of 4?) (**Hint**: Consider the order of $a^x \bmod p$ and use problem 43b).)

Practice Problems: **2.17**, **2.28**,

Examples of Discrete Logarithm Calculations

Let $p = 401$ with primitive root $g = 3$. What is the discrete logarithm of 11, i.e. find e such that $3^e \equiv 11 \pmod p$. In GAP we can use:

```
gap> p:=401;g:=3;
401
3
gap> RootInt(401);
20
gap> a:=RootInt(401)+1;
21
gap> giant:=List([0..a],
     x->PowerMod(g,x*a,p));
[1, 335, 346, 21, 218, 48, 40, 167,
 206, 38, 299, 316, 397, 264, 220,
 317, 331, 209, 241, 134, 379, 249]
gap> ginv:=g^-1 mod p; #Inverse
134
gap> baby:=List([0..a],
    x->PowerMod(ginv,x,p)*11 mod p);
[11,271,224,342,114,38,280,227,343,
 248,350,384,128,310,237,79,160,187,
 196,199,200,334 ]
gap> Intersection(giant,baby);
[ 38 ]
gap> Position(giant,38);
10
gap> Position(baby,38);
6
```

```
gap> e:=(10-1)*a+6-1;
194
gap> PowerMod(g,e,p); # test
11
```

For a larger example, find the discrete logarithm of 1234 to base 2 modulo 10130699:

```
gap> p:=10130699;;g:=2;;
gap> a:=RootInt(p)+1;
3183
gap> giant:=List([0..a],
         x->PowerMod(g,x*a,p));
[ 1, 498324, 3115088, 6235441,
  ...
  9420722 ]
gap> ginv:=g^-1 mod p;
5065350
gap> baby:=List([0..a],x->
 PowerMod(ginv,x,p)*1234 mod p);;
[ 1234, 617, 5065658,  ...
gap> Intersection(giant,baby);;
[ 2199948 ]
gap> Position(giant,2199948);
964
gap> Position(baby,2199948);
189
gap> e:=(964-1)*a+189-1;
3065417
gap> PowerMod(g,e,p);
1234
```

Pohlig-Hellman Example We want to find the discrete logarithm of 13 to base 2 modulo $p = 10099$. We use the coprime factorization $p - 1 = 297 \cdot 34 = (3^3 11)(2 \cdot 17)$. Note that $\mathrm{OrderMod}_p(13) = (3^2 \cdot 11)(2 \cdot 17)$.

```
gap> p:=10099;;g:=2;;
gap> Factors(OrderMod(13,p));
[ 2, 3, 3, 11, 17 ]
```

We first form powers of 2 that have orders $3^3 11$, respectively $2 \cdot 17$ and also powers of 13 that are of order $3^2 11$, respectively $2 \cdot 17$:

```
gap> a:=PowerMod(2,34,p);
5829
gap> OrderMod(a,p);
297
gap> b:=PowerMod(2,27*11,p);
6962
gap> c:=PowerMod(13,34,p);
9262
gap> d:=PowerMod(13,99,p);
5756
```

For later use we determine that $13 \equiv c^{67} d^{11} \pmod{p}$

```
gap> GcdRepresentation(34,99);
[ -32, 11 ]
gap> -32 mod 99;
67
```

Now we solve two discrete logarithm problems: c as power of a, using that $\mathrm{OrderMod}_p(a) = 297$.

```
gap> root:=RootInt(297);
17
gap> giant:=List([0..root],
       x->PowerMod(a,x*root,p));;
gap> ainv:=a^-1 mod p;;
gap> baby:=List([0..root],
      x->PowerMod(ainv,x,p)*c mod p);;
gap> is:=Intersection(giant,baby)[1];
6148
gap> (Position(giant,is)-1)*root
        +Position(baby,is)-1;
78
```

Similarly we find that $b^{19} \equiv d \pmod{p}$:

```
gap> root:=RootInt(OrderMod(b,p));
5
gap> giant:=List([0..root],
       x->PowerMod(b,x*root,p));
[ 1, 7890, 1864, 2816, 440, 7643 ]
gap> binv:=b^-1 mod p;;
gap> baby:=List([0..root],
      x->PowerMod(binv,x,p)*d mod p);
```

```
[ 5756, 3137, 10098, 2833, 2816, 482 ]
gap> is:=Intersection(giant,baby)[1];;
gap> (Position(giant,is)-1)*root
        +Position(baby,is)-1;
19
```

Together this gives that

$$13 \equiv c^{67}d^{11} \equiv (a^{78})^{67}(b^{19})^{11} \equiv \left(\left(2^{34}\right)^{78}\right)^{67}\left(\left(2^{297}\right)^{19}\right)^{11}$$
$$\equiv 2^{34\cdot 78\cdot 67+297\cdot 19\cdot 11} \equiv 2^{239757} \equiv 2^{7503} \pmod{p}$$

(using that $7503 \equiv 239757 \pmod{(p-1)}$). We verify:

```
gap> (34*78*67+297*19*11) mod (p-1);
7503
gap> PowerMod(2,7503,p);
13
```