SOLUTIONS
Math 345
Homework 8
11/1/2017

a	0	1	2	3	4	5	6	7	8	9	10	11
2^a	1	2	4	8	16	32	64	128	256	512	1024	2048

Exercise 29. Computing $5^n \pmod{1147}$. Note that $1147 = 31 * 37$.

(a) Verify $\gcd(5, 1147) = 1$. What does Euler's formula tell us for powers of 5 modulo 1147?

Answer. The Euclidean algorithm produces

a	b	q	r
1147	5	229	2
229	2	114	1
114	1	114	0

, so $\gcd(5, 1147) = 1$.

This means that $1 \equiv_{1147} 5^{\phi(1147)}$, where $\phi(1147) = 30 * 36 = 1080$.

□

(b) Using successive squaring, compute a table of $5^{(2^a)} \pmod{1147}$ (reducing at each step). According to part (a), how high must your table go?

Answer. We don't need to compute powers higher than 1080, so our table only needs to go up to $5^{2^{10}}$. By successive squaring, we get the following.

a	$\overline{5^{2^{a-1}}}^2$	$5^{2^a} \pmod{1147}$
0	5	5
1	25	25
2	625	625
3	390625	645
4	416025	811
5	657721	490
6	240100	377
7	142129	1048
8	1098304	625
9	390625	645
10	416025	811

□

(c) For $n = 10, \quad 1200$, and $10,000$:

(i) Use Euler's formula, if possible, to reduce $5^n \pmod{1147}$ to a smaller problem if possible. Let m be the resulting power such that $5^m \equiv_{1147} 5^n$.

(ii) Rewrite m in base 2.

(iii) Use your table in part (b) to reduce $5^m \pmod{1147}$ into a smaller product.

(iv) Use successive reduction of your product to compute a value $1 \leq x < 1147$ such that $x \equiv_{1147} 5^n$.

Answer. For $n = 10$:

(i) The least residue modulo 1080 is $m = 10$.

(ii) Rewriting $m = 10$ in base 2 gives $10 = 2^3 + 2$.

(iii) Using our table in part (b) to reduce $5^{10} \pmod{1147}$ gives

$$5^{10} = 5^{2^3} * 5^2 \equiv_{1147} 645 * 25.$$

(iv) Using successive reduction of our product, there is only one step:

$$5^{10} \equiv_{1147} 645 * 25 = 16125 \equiv_{1147} \boxed{67}.$$

For $n = 1200$:

(i) We have $1200 \equiv_{1080} 120$.

(ii) Rewriting 120 in base 2 gives

$$120 = 64 + 32 + 16 + 8 = 2^6 + 2^5 + 2^4 + 2^3.$$

(iii) Using our table in part (b) to reduce $5^{120} \pmod{1147}$ gives

$$5^{120} = 5^{2^6} * 5^{2^5} * 5^{2^4} * 5^{2^3} \equiv_{1147} 377 * 490 * 811 * 645.$$

(iv) Using successive reduction of our product gives

$$\begin{aligned} 5^{1200} \equiv_{1147} 5^{120} &\equiv_{1147} 377 * 490 * 811 * 645 \\ &\equiv_{1147} 63 * 811 * 645 && \text{since } 377 * 490 \equiv_{1147} 63, \\ &\equiv_{1147} 625 * 625 && \text{since } 63 * 811 \equiv_{1147} 625, \\ &\equiv_{1147} \boxed{645}. \end{aligned}$$

For $n = 10,000$:

(i) The least residue of $10,000$ modulo 1080 is $m = 280$.

(ii) Rewriting 280 in base 2 gives

$$280 = 256 + 16 + 8 = 2^8 + 2^4 + 2^3.$$

(iii) Using our table in part (b) to reduce $5^{280} \pmod{1147}$ gives

$$5^{280} = 5^{2^8} * 5^{2^4} * 5^{2^3} \equiv_{1147} 625 * 811 * 645.$$

(iv) Using successive reduction of our product gives

$$625 * 811 * 645 \equiv_{1147} 1048 * 645 \equiv_{1147} \boxed{377}.$$

□

Exercise 30. Repeat the previous exercise for $7^n \pmod{1375}$. Note that $1375 = 5^3 \cdot 11$.

(a) Verify $\gcd(7, 1375) = 1$. What does Euler's formula tell us for powers of 7 modulo 1375?

Answer. The Euclidean algorithm produces

a	b	q	r
1375	7	196	3
196	3	65	1
65	1	65	0

, so $\gcd(7, 1375) = 1$.

This means that $1 \equiv_{1375} 7^{\phi(1375)}$, where $\phi(1375) = 5^2 * 4 * 10 = 1000$. □

(b) Using successive squaring, compute a table of $7^{(2^a)} \pmod{1375}$ (reducing at each step). According to part (a), how high must your table go?

Answer. We don't need to compute powers higher than 1000, so our table only needs to go up to 5^{2^9}. By successive squaring, we get the following.

a	$\overline{5^{2^{a-1}}}^2$	$5^{2^a} \pmod{1375}$
0	7	7
1	49	49
2	2401	1026
3	1052676	801
4	641601	851
5	724201	951
6	904401	1026
7	1052676	801
8	641601	851
9	724201	951

□

(c) For $n = 10, \quad 1200$, and $10,000$:

(i) Use Euler's formula, if possible, to reduce $7^n \pmod{1375}$ to a smaller problem if possible. Let m be the resulting power such that $7^m \equiv_{1375} 7^n$.

(ii) Rewrite m in base 2.

(iii) Use your table in part (b) to reduce $7^m \pmod{1375}$ into a smaller product.

(iv) Use successive reduction of your product to compute a value $1 \leq x < 1375$ such that $x \equiv_{1375} 7^n$.

Answer. For $n = 10$:

(i) The least residue modulo 1000 is $m = 10$.

(ii) Rewriting $m = 10$ in base 2 gives $10 = 2^3 + 2$.

(iii) Using our table in part (b) to reduce $5^{10} \pmod{1147}$ gives

$$7^{10} = 7^{2^3} * 7^2 \equiv_{1375} 801 * 49.$$

(iv) Using successive reduction of our product, there is only one step:

$$7^{10} \equiv_{1375} 801 * 49 = 39249 \equiv_{1375} \boxed{749}.$$

For $n = 1200$:

(i) We have $1200 \equiv_{1000} 200$.

(ii) Rewriting 200 in base 2 gives

$$200 = 128 + 64 + 8 = 2^7 + 2^6 + 2^3.$$

(iii) Using our table in part (b) to reduce $7^{200} \pmod{1375}$ gives

$$7^{200} = 7^{2^7} * 7^{2^6} * 7^{2^3}.$$

Note that $7^{2^7} \equiv_{1375} 7^{2^3}$, so $7^{2^7} * 7^{2^3} \equiv_{1375} 2^4$. So

$$7^{200} = 7^{2^6} * 7^{2^4} \equiv_{1375} 1026 * 851.$$

(iv) Using successive reduction of our product, there is only one step:

$$7^{1200} \equiv_{1375} 7^{200} \equiv_{1375} 1026 * 851 = 873126 \equiv_{1375} 1.$$

For $n = 10,000$: The least residue of $10,000$ modulo 1000 is 0, so $7^{10000} \equiv_{1375} 1$. □

Exercise 31. Prime testing.

(a) Compute $7^{7386} \pmod{7387}$ by the method of successive squaring. Is 7387 prime?

Answer. We have

$$\begin{aligned} 7386 &= 4096 + 2048 + 1024 + 128 + 64 + 16 + 8 + 2 \\ &= 2^{12} + 2^{11} + 2^{10} + 2^7 + 2^6 + 2^4 + 2^3 + 2. \end{aligned}$$

Using successive squaring we get the following:

a	$\overline{7^{2^{a-1}}}^2$	$7^{2^a} \pmod{7387}$
0	7	7
1	49	49
2	2401	2401
3	5764801	2941
4	8649481	6691
5	44769481	4261
6	18156121	6262
7	39212644	2448
8	5992704	1847
9	3411409	6002
10	36024004	4992
11	24920064	3713
12	13786369	2227

So

$$\begin{aligned} 7^{7386} &= 7^{2^{12}} * 7^{2^{11}} * 7^{2^{10}} * 7^{2^7} * 7^{2^6} * 7^{2^4} * 7^{2^3} * 7^2 \\ &\equiv_{7387} 2227 * 2227 * 4992 * 2448 * 6262 * 6691 * 2941 * 49 \\ &\equiv_{7387} 2852 * 2318 * 7365 * 3756 \\ &\equiv_{7387} 6958 * 6012 \equiv_{7387} 6302 \not\equiv_{7387} 1. \end{aligned}$$

So 7387 is not prime. □

(b) Compute $7^{7392} \pmod{7393}$ by the method of successive squaring. Is 7393 prime?

Answer. We have

$$\begin{aligned} 7392 &= 4096 + 2048 + 1024 + 128 + 64 + 32 \\ &= 2^{12} + 2^{11} + 2^{10} + 2^7 + 2^6 + 2^5. \end{aligned}$$

Using successive squaring we get the following:

a	$\overline{7^{2^{a-1}}}^2$	$7^{2^a} \pmod{7393}$
0	7	7
1	49	49
2	2401	2401
3	5764801	5654
4	31967716	384
5	147456	6989
6	48846121	570
7	324900	7001
8	49014001	5804
9	33686416	3908
10	15272464	5919
11	35034561	6527
12	42601729	3263

So

$$\begin{aligned} 7^{7392} &= 7^{2^{12}} * 7^{2^{11}} * 7^{2^{10}} * 7^{2^7} * 7^{2^6} * 7^{2^5} \\ &\equiv_{7393} 3263 * 6527 * 5919 * 7001 * 570 * 6989 \\ &\equiv_{7393} 5761 * 1154 * 6296 \\ &\equiv_{7393} 1887 * 6296 \equiv_{7387} 1. \end{aligned}$$

So 7393 may or may not be prime. □