Math 345 – Wednesday 10/25/17

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?

(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?

(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 $x \equiv_{1147} 5^n$.

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

Exercise 31. Prime testing.

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

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