Exercise Set 3:
Integers Modulo n

Math 414, Winter 2010, University of Washington

Due Wednesday, January 27, 2010

1. Let n be a positive integer and let

$$P = \{a : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

Is it necessarily the case that

$$\prod_{a \in P} a \equiv -1 \pmod{n}?$$

Answer: Nope. E.g., for $n = 8$ we have $1 \cdot 3 \cdot 5 \cdot 7 \equiv 1 \pmod{8}$.

Some relevant Sage code:

```
sage: def f(n): return prod([Mod(a,n) for a in [1..n] if gcd(a,n) == 1])
sage: for n in [2..10]: print n, f(n)
2 1
3 2
4 3
5 4
6 5
7 6
8 1
9 8
10 9
```

2. (a) Find an integer x such that

$$x \equiv 3 \pmod{7} \quad \text{and} \quad x \equiv 5 \pmod{11}.$$

Answer: -39. Relevant Sage code:

```
sage: x = CRT(3,5,7,11); x
-39
sage: x%7
3
sage: x%11
5
```

(b) Find an integer x such that

$$x \equiv -1 \pmod{2010} \quad \text{and} \quad x \equiv 1 \pmod{2011}.$$

Answer: -4021

```
sage: x = CRT(-1,1,2010,2011); x
-4021
sage: x%2010
2009
sage: x%2011
1
```

3. Find all *four* solutions to the equation

$$x^2 - 1 \equiv 0 \pmod{100}.$$

Answer: 1,49,51, 99. Relevant code:

```
sage: [x for x in Integers(100) if x^2 == 1]
[1, 49, 51, 99]
```

4. Suppose that $n > 1$ is an integer and that $2^{n-1} \equiv -1 \pmod{n}$. Is it possible that n is prime?

Answer: Nope, n *can't be prime. If* n *were prime, then* $2^{n-1} \equiv 1 \pmod{n}$ *by Fermat's Little Theorem. So if the above condition also holds, we have* $-1 \equiv 1 \pmod{n}$, *which implies that* $n = 2$. *However,* $2^{2-1} \equiv 2 \pmod{2}$ *so the above condition is not satisfies by* 2.

5. Find an integer x such that $5x + 7 \equiv 2010 \pmod{2011}$. *Answer:* 1205. *Relevant code:*

```
Find it:
    sage: x = (Mod(2010,2011) - Mod(7,2011))/Mod(5,2011); x
    1205
```

Double check that it works:

```
sage: Mod(5*x + 7 , 2011)
2010
```