HW 6
Due: Friday, October 25

§4.6/6, 7; §3.13/17, 18, 21, 24, 26; and the following Python problem:

Write a program `suntzu` which on input `a, b, m, n` with $\gcd(m,n) = 1$, computes the smallest nonnegative x for which $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. You do not have to check that $\gcd(m,n) = 1$. Use your code to compute the following:

(a) `suntzu(1, 3, 17, 19)`

(b) `suntzu(17, 21, 1452817, 3829183)`

4.6.6 If r is random, then the probability of drawing from the list is equal to the number of elements on the list, N, over the total number of bit strings, 2^M. This gives the first probability.

For the second, if r is pseudorandom, then by definition r is on the list, so the probability is 1.

For (b): $P(r \text{ is random}) = \frac{1}{2}$ according to the rules of the R game, and same with psuedorandom. The first and third equalities now follow from part (a) and the definition of conditional probability—so, for instance,

$$P(r \text{ is random} \cap r \text{ is on the list}) = P(r \text{ is random})P(r \text{ is on the list} | r \text{ is random}).$$

For the 2nd, observe that the sum of the first two probabilities must equal $P(r \text{ is random}) = \frac{1}{2}$, and so the 2nd probability works out. The 4th is similar.

For (c): She wins in two cases: r is random and r is not on the list, or r is pseudorandom. These are disjoint cases, so we can add the probabilities. The claim follows from (b).

For (d): This is just substitution into (c).

3.13.21a We wish to solve

$$x^2 \equiv 133 \pmod{11} \text{ and } x^2 \equiv 133 \pmod{13}.$$

The first congruence is the same as $x^2 \equiv 1 \pmod{11}$, so $x \equiv \pm 1 \pmod{11}$.

The second congruence is equivalent to $x^2 \equiv 3 \pmod{13}$. We can use brute force to solve this one, or observe that $4^2 = 16 \equiv 3 \pmod{13}$, so $x \equiv \pm 4 \pmod{13}$. Now we invoke Sun Tzu's Theorem; or better yet, the code from (a):

```
suntzu(1,4,11,13)
suntzu(-1,-4,11,13)
suntzu(1,-4,11,13)
suntzu(-1,4,11,13)
```

These yield the solutions $56, 87, 100, 43 \pmod{143}$.

A. Here is one solution

```
def suntzu(a, b, m, n):
    """Compute solution to x = a mod m, = b mod n."""
    d, r, s = egcd(m,n)
    return (b*r*m + a*s*n)%(m*n)
```

The last mod mn is necessary to get the smallest nonnegative value. The correct values are (a) 307 and (b) 3202429984947.