Homework 23, due October 28

(1) Let $n = 1042387$. Factor $t^2 - n$ for

$$t = 1021, 1027, 1030, 1061, 1112, 1129, 1148, 1175, 1217, 1390, 1520.$$

Make a matrix (as in section 6.4.1) and find at least two linear dependencies $\pmod 2$ among the rows. Use this information to factor n. Explain your work.

(2) Let $n = 527773$. Calculate the values of the polynomial $f(x) = (x + \lfloor\sqrt{n}\rfloor)^2 - n$ for x from -17 to 17 and factor them. (Remember that primes p with $\left(\frac{n}{p}\right) = -1$ will never divide $f(x)$.) Use this information to find some squares that factor into small primes $\pmod n$, and use this information to factor n. Explain your work.

(3) Bob's public RSA key is $(n, e) = (47198353746711821023370804532488820972149852741 3, 37)$. You have reason to believe that Bob has a fairly weak RSA key. You intercept a message intended for Bob:

`2759787038814454200682773100274065167994289953 6`

Decrypt. Explain how you did it.