Homework 16, due October 13

(1) Find a rational approximation p/q to $\alpha = \sqrt{2} + e + \pi$ such that $|\alpha - p/q| < 10^{-14}$ and $q < 1.5 \cdot 10^7$.

(2) A message, with corresponding ciphertext

```
c = 399339999714121134263218574566850518529794061938465942381076754 74\
6401249484393554050708152388260422760810117132571729535475464500130 47\
116420236573561714197,
```

was encrypted with the public key

```
(n,e) = (735949021753953348445321809558616397418695897742383880582800 5\
4677303127811125010639459930983002184507320932224006318815479009843600\
3564681620225342617878 61, 638012627091397751315380695548991528112423 04\
5489885458408934082491728415514326044234606203325356953193732297565154\
6736731071992465103056521824829415832628 9).
```

Decrypt.

(3) (Håstad's broadcast attack with $e = 3$) Alice wants to send a message m to her friends Bob, Carol, and David. Bob, Carol, and David have RSA public keys (n, e) given by $(n_B, 3), (n_C, 3)$, and $(n_D, 3)$, respectively, where n_B, n_C, n_D are distinct (so they have different public moduli but the same encryption exponent). Assume that

$$1 \leq m < \min(n_B, n_C, n_D).$$

If Eve observes Alice sending ciphertexts $c_B \equiv m^3 \pmod{n_B}, c_C \equiv m^3 \pmod{n_C}, c_D \equiv m^3 \pmod{n_D}$ to Bob, Carol, and David, respectively, show that Eve can recover m in the following manner.

(a) Show that, if any of n_B, n_C, n_D have a factor in common, then Eve can recover m by factoring.

(b) By part (a), we may assume n_B, n_C, n_D are pairwise coprime. Show that Eve can use the Chinese Remainder Theorem to find $y \pmod{n_B n_C n_D}$ with

$$y \equiv c_B \pmod{n_B}, \qquad y \equiv c_C \pmod{n_C}, \qquad y \equiv c_D \pmod{n_D}.$$

(c) Show that Eve may actually take $y = m^3$, so that Eve can recover m by taking a cube root in the integers.