Math 116 Spring 2022
Homework 5-2
Due Friday, May 13th

Problem 1. (3.22) Use Pollard's $p-1$ method to factor each of the following numbers.

(a) $n = 1739$

(b) $n = 220459$

Show your work and indicate which prime factor p of n has the property that $p-1$ is a product of small primes.

Problem 2. (3.27) Compute the following values of $\Psi(X, B)$, the number of B-smooth numbers between 2 and X (see page 150).

(a) $\Psi(25, 3)$

(b) $\Psi(35, 5)$

(c) $\Psi(50, 7)$

Problem 3. (3.26(b)) Our goal is to factor $N = 52907$. Use the data provided to find values of a and b satisfying $a^2 \equiv b^2 \pmod{N}$ by hand. Then use Sage to compute $\gcd(N, a-b)$ in order to find a nontrivial factor of N

$$\begin{array}{llll}
399^2 \equiv 480 & \pmod{52907} & \text{and} & 480 = 2^5 \cdot 3 \cdot 5 \\
763^2 \equiv 192 & \pmod{52907} & \text{and} & 192 = 2^6 \cdot 3 \\
773^2 \equiv 15552 & \pmod{52907} & \text{and} & 15552 = 2^6 \cdot 3^5 \\
976^2 \equiv 250 & \pmod{52907} & \text{and} & 15552 = 2 \cdot 5^3
\end{array}$$

Problem 4. (3.37) Let p be an odd prime and let a be an integer not divisible by p.

(a) Prove that $a^{(p-1)/2}$ is congruent to either 1 or -1 modulo p.

(b) Prove that $a^{(p-1)/2}$ is congruent to 1 modulo p if and only if a is a quadratic residue modulo p. (*Hint.* Let g be a primitive root for p and use the fact, proven during the course of proving Proposition 3.61, that g^m is a quadratic residue if and only if m is even.)

Problem 5. Decide whether 35 is a quadratic residue modulo the prime 101 by computing the Legendre symbol by hand.

Problem 6. (3.42(a)(c), with Sage) Perform the following encryptions and decryptions using the Goldwasser– Micali public key cryptosystem (Table 3.9).

(a) Bob's public key is the pair $N = 1842338473$ and $a = 1532411781$. Alice encrypts 3 bits and sends Bob the ciphertext blocks

$$1794677960, \quad 525734818, \quad \text{and} \quad 420526487.$$

Decrypt Alice's message using the factorization

$$N = pq = 32411 \cdot 56843.$$

(b) Bob's public key is $N = 781044643$ and $a = 568980706$. Encrypt the 3 bits 1, 1, 0 using, respectively, the three "random" values

$$r = 705130839, \quad r = 631364468, \quad r = 67651321.$$

Note that in Sage, `kronecker(a,p)` returns the Legendre symbol $\left(\frac{a}{p}\right)$.

Problem 7. (4.1, with Sage) Samantha uses the RSA signature scheme with primes $p = 541$ and $q = 1223$ and public verification exponent $e = 159853$.

(a) What is Samantha's public modulus? What is her private signing key?

(b) Samantha signs the digital document $D = 630579$. What is the signature?

Problem 8. (4.2, with Sage) 4.2. Samantha uses the RSA signature scheme with public modulus N = 1562501 and public verification exponent e = 87953. Adam claims that Samantha has signed each of the documents

$$D = 119812, \quad D' = 161153, \quad D'' = 586036,$$

and that the associated signatures are

$$S = 876453, \quad S' = 870099, \quad S'' = 602754.$$

Which of these are valid signatures?