Math 4981 Spring 2021
Cryptography HW 8 Solutions
Due Thursday, March 11

1. Use the Euclidean Algorithm to compute $\gcd(5320, 2156)$.

   Solution:

$$\begin{aligned} 5320 &= 2 \cdot 2156 + 1008 & r_2 &= 1008 \\ 2156 &= 2 \cdot 1008 + 140 & r_3 &= 140 \\ 1008 &= 7 \cdot 140 + 28 & r_4 &= 28 \\ 140 &= 5 \cdot 28 + 0 & r_5 &= 0 \end{aligned}$$

   so $\gcd(5320, 2156) = 28$.

2. If n is a positive integer, use the Euclidean algorithm to find $\gcd(2n^2 + 6n - 4, 2n^2 + 4n - 3)$.

   Solution:

$$\begin{aligned} r_0 = 2n^2 + 6n - 4 \qquad & r_1 = 2n^2 + 4n - 3 \\ 2n^2 + 6n - 4 = 1 \cdot (2n^2 + 4n - 3) + 2n - 1 \qquad & r_2 = 2n - 1 \\ 2n^2 + 4n - 3 = (n + 2) \cdot (2n - 1) + n - 1 \qquad & r_3 = n - 1 \\ 2n - 1 = 2(n - 1) + 1 \qquad & r_4 = 1 \\ n - 1 = (n - 1) \cdot 1 + 0 \qquad & r_5 = 0 \end{aligned}$$

   so $\gcd(2n^2 + 6n - 4, 2n^2 + 4n - 3) = 1$.

3. Use Pollard's $p - 1$ method to factor 1517. Show all your steps.

   Solution:

   We'll take $a_1 = 2$, and then:

   - $a_2 = 2^2 = 4$, and $\gcd(3, 1517) = 1$.
   - $a_3 = 4^3 = 64$, and $\gcd(63, 1517) = \gcd(63, 5) = 1$.
   - $a_4 = 64^4 = 16777216 \equiv 712 \mod 1517$, and $\gcd(712, 1517) = \gcd(712, 93) = \gcd(93, 61) = \gcd(61, 32) = 1$.

- $a_5 \equiv 712^5 \equiv 1394 \mod 1517$, and $\gcd(1517, 1394) = \gcd(1394, 123) = \gcd(123, 41) = 41$.

Thus 41 is a non-trivial factor of 1517. The other factor, we see, is 37.

4. Use the Discrete Logarithm factoring algorithm to factor 3403, using the fact that $\log_2(1) = 820$ modulo 3403. (I know you could factor this directly, but use the discrete logarithm algorithm and explain the steps you're using.)

   Solution: We have $r = 820$ so $r/2 = 410$. We compute $2^{410} \equiv 3238 \mod 3403$ which is not ± 1. So we compute $\gcd(3237, 3403) = 83$ and $\gcd(3239, 3403) = 41$, and thus we conclude that $3403 = 83 \cdot 41$.

5. The group S_3 is the set $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, where e is the identity and multiplication obeys the following rules: $\sigma^3 = e = \tau^2, \tau\sigma = \sigma^2\tau$.

   (a) What are σ^{-1} and τ^{-1}? That is, tell me which of the six elements in the set I gave you is σ^{-1} and which is τ^{-1}.

   (b) Compute $\tau\sigma^2, \tau(\sigma\tau), (\sigma\tau)(\sigma\tau)$, an $(\sigma\tau)(\sigma^2\tau)$. (Again, your answer for each part should be one of the six elements I gave you.)

   Solution:

   (a) $\sigma^{-1} = \sigma^2$ and $\tau^{-1} = \tau$.

   (b)

$$\begin{aligned}
\tau\sigma^2 &= \sigma^2\tau\sigma = \sigma^4\tau = \sigma\tau \\
\tau\sigma\tau &= \sigma^2\tau\tau = \sigma^2 \\
\sigma\tau\sigma\tau &= \sigma\sigma^2\tau\tau = \sigma^3\tau^2 = ee = e \\
\sigma\tau\sigma^2\tau &= \sigma\sigma\tau\tau = \sigma^2.
\end{aligned}$$

6. Let $m > 2$ be a positive integer. Prove that $\mathbb{Z}/m\mathbb{Z}^\times$ with the operation of multiplication is an abelian group. (Non-obvious thing to check: is multiplication a binary operation? That is, if you multiply two elements together, do you get another?)

   Solution:

   First, we check that this is a binary operation. Suppose $a, b \in \mathbb{Z}/m\mathbb{Z}^\times$. Then ab is an integer and can be viewed as an integer $\mod m$. We know that a and b are both invertible, because that's the definition of $\mathbb{Z}/m\mathbb{Z}^\times$; then we know that $b^{-1}a^{-1}$ is an inverse to ab, so $ab \in \mathbb{Z}/m\mathbb{Z}^\times$.

   Then we just need to check: there's an identity $1 \in \mathbb{Z}/m\mathbb{Z}^\times$, such that $1 \cdot a = a$ for any $a \in \mathbb{Z}/m\mathbb{Z}^\times$. Each $a \in \mathbb{Z}/m\mathbb{Z}^\times$ has an inverse by definition of $\mathbb{Z}/m\mathbb{Z}^\times$. And we know that for any integers a, b, c, then $(ab)c = a(bc)$, and thus $(ab)c \equiv a(bc) \mod m$.

   Finally, we need to check this is an *abelian* group. But for any integers a, b, we know that $ab = ba$, and thus $ab \equiv ba \mod m$.

   (We're actually sort of skipping over a step here, that multiplication is well-defined. We maybe should check that if $a \equiv b$ and $c \equiv d$ then $ac \equiv bd$. But we're taking that as given from the work we've already done with $\mathbb{Z}/m\mathbb{Z}$.)