Homework 4

1. *Show that $8n+3$ and $5n+2$ are relatively prime for all integers n.*

   We first use the fact that $(a,b) = (a+kb, b)$ applied to $a = 8n+3$, $b = 5n+2$, and $k = -1$ to find that $(8n+3, 5n+2) = (3n+1, 5n+2)$.

   Then, we apply the same fact, but with $a = 5n+2$, $b = 3n+1$, and $k = -1$ to find $(3n+1, 5n+2) = (3n+1, 2n+1)$.

   Finally, we apply the fact again twice more to get $(3n+1, 2n+1) = (n, 2n+1) = (n, 1) = 1$. Therefore, $(8n+3, 5n+2) = 1$, so $8n+3$ and $5n+2$ are relatively prime.

2. *Using Euclid's proof that there are infinitely many primes (this is the first proof we gave in class), show that the* n*th prime,* p_n*, does not exceed* $2^{2^{n-1}}$ *for* $n \geqslant 1$*. Conclude that when* n *is a positive integer, there are at least* $n+1$ *primes less than* 2^{2^n}*. Conclude that for integers* x *of the form* 2^{2^n}*,* $\pi(x) \geqslant \log_2 \log_2 x$

   We prove this by strong induction on n. Note that for $n = 1$, $p_n = 2$ and $2^{2^{n-1}} = 2$, so $p_n \leqslant 2^{2^{n-1}}$.

   Now, if $p_k \leqslant 2^{2^{k-1}}$, we aim to show that $p_{n+1} \leqslant 2^{2^n}$. By Euclid's proof that there are infinitely many primes, $p_{n+1} \leqslant p_1 \cdots p_n + 1$. By the induction hypotheses, $p_1 \cdots p_2 \leqslant 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}}$, so

$$p_{n+1} \leqslant p_1 \cdots p_n + 1 \leqslant 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 = 2^{2^0+2^1+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 < 2^{2^n}$$

   Hence, if n is a positive integer, then $p_1, \ldots, p_{n+1} \leqslant 2^{2^n}$, so there are at least $n+1$ primes less than or equal to 2^{2^n}. Substituting $x = 2^{2^n}$, we have $\pi(x) \geqslant n + 1 = \log_2 \log_2 x + 1 \geqslant \log_2 \log_2 x$.

3. *Show that if* $n \in \mathbb{Z}_{>1}$ *and* $i, j \in \mathbb{N}$ *satisfying* $1 \leqslant i < j \leqslant n$*, then*

$$(n! \cdot i + 1, n! \cdot j + 1) = 1$$

Hint: You may use the fact that if p *is prime and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

We apply the fact that $(a, b) = (a + bc, b)$ with $a = n! \cdot j + 1$, $b = n! \cdot i + 1$, and $c = -1$. Hence $(n! \cdot i + 1, n! \cdot j + 1) = (n! \cdot i + 1, n! \cdot (j - i))$.

Now if p is a prime factor of $n! \cdot (j - i)$, then $p \mid n!$ or $p \mid (j - i)$. If $p \mid n!$, then $p \leqslant n$. If $p \mid (j - i)$, then $p \leqslant j - i < n$. In either case, $p \leqslant n$.

If p is a prime factor of $n! \cdot i + 1$, then $p > n$ (otherwise, if $p \leqslant n$, then $p \mid n! \cdot i$ and $p \mid n! \cdot i + 1$, a contradiction).

Hence, $n! \cdot i + 1$ and $n! \cdot (j - i)$ share no prime factors, so

$$(n! \cdot i + 1, n! \cdot j + 1) = (n! \cdot i + 1, n! \cdot (j - i)) = 1$$

4. *Show that if $a^k - 1$ is prime (with $a \geqslant 1$ and $k \geqslant 2$), then...*

   (a) $\ldots a = 2$

   Suppose that $a \geqslant 1$ and $k \geqslant 2$. If $a = 1$, then $a^k - 1 = 0$, which is not prime, so we may assume that $a \geqslant 2$. Then

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$$

   If $a > 2$, then we see that $a^k - 1$ is not prime because $(a-1) \mid (a^k - 1)$ and $1 < a - 1 < a^k - 1$. Therefore, $a = 2$.

   (b) $\ldots k$ *is prime*

   To show that if $2^k - 1$ is prime, then k is prime, we prove the contrapositive. Suppose that k is not prime, so that there exists an integer a so that $1 < a < k$ and $a \mid k$. Then we observe that

$$\begin{aligned}
2^k - 1 &= 2^{k-1} + 2^{k-2} + \cdots + 2 + 1 \\
&= \sum_{i=0}^{k/a} \sum_{j=1}^{a} 2^{k-ai-j} \\
&= \sum_{i=0}^{k/a} 2^{k-a(i-1)} \sum_{j=1}^{a} 2^{a-j} \\
&= \sum_{i=0}^{k/a} 2^{k-a(i-1)} \cdot (2^a - 1) \\
&= (2^a - 1) \sum_{i=0}^{k/a} 2^{k-a(i-1)}
\end{aligned}$$

   so $2^a - 1$ is a factor of $2^k - 1$. Since $1 < a < k$, we have that $1 < 2^a - 1 < 2^k - 1$ and so $2^k - 1$ is not prime.