Solution Sheet 5

1. ★ Primes up to 200:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	
101		103		107	109
		113			
				127	
131				137	139
					149
151				157	
		163		167	
		173			179
181					
191		193		197	199

Thus $\pi(200) = 46$.

The smallest prime not in the table is 211. So $211^2 = 44521$ is the smallest composite integer that has no prime factor in the table.

(i) $44517 = 3 \times 11 \times 19 \times 71$,

(ii) $44503 = 191 \times 233$, (I hope you started looking for prime factors near 200 rather than 2.)

(iii) 44519 is prime. If composite it would have a prime factor $\leq \sqrt{44519}$, i.e. less than 210 and thus be in the table. It should have taken you 46 "trial divisions" to find that none of the 46 primes divided 44519 and thus it was, itself, prime.

2. (i) $(7,11,13)$, $(13,17,19)$, $(37,41,43)$ and $(67,71,73)$.

   (ii) We will show that if $p \equiv 1$ or $2 \bmod 3$ then at least one of $p, p+3$ and $p+4$ is a multiple of 3 and thus not prime.

   Consider three cases.

   a) If $p \equiv 1 \bmod 3$, i.e. $p = 1+3k$, then $p+2 = 3(1+k)$ is not prime.
   b) If $p \equiv 2 \bmod 3$, i.e. $p = 2+3k$, then $p+4 = 3(2+k)$ is not prime.
   c) If $p \equiv 0 \bmod 3$, then the only prime divisible by 3 is 3. This leads to the given triplet of $(3,5,7)$.

3. ★ (i) We have $5555 \equiv 4 \bmod 7$ and $(4,7) = 1$ and so, by Fermat's Little Theorem, $4^6 \equiv 1 \bmod 7$. But $2222 = 370 \times 6 + 2$. Thus

$$5555^{2222} \equiv \left(4^6\right)^{370} 4^2 \equiv 1^{370} 16 \equiv 2 \bmod 7.$$

   We also have $2222 \equiv 3 \bmod 7$ and $(3,7) = 1$ and so, by Fermat's Little Theorem, $3^6 \equiv 1 \bmod 7$. But $5555 = 925 \times 6 + 5$. So

$$\begin{aligned} 2222^{5555} &\equiv \left(3^6\right)^{925} 3^5 \equiv 1^{925} \times 9 \times 9 \times 3 \\ &\equiv 2 \times 2 \times 3 \\ &\equiv 5 \bmod 7. \end{aligned}$$

   Hence
$$5555^{2222} + 2222^{5555} \equiv 2 + 5 \equiv 0 \bmod 7.$$

   (ii) We immediately examine $5555^{2222} + 2222^{5555} \bmod 9$, **not** $\bmod 3$. Because 9 is not prime we need to use Euler's Theorem which, in this case, says that if $\gcd(a,9) = 1$, then $a^{\phi(9)} \equiv 1 \bmod 9$. Simply by listing the integers less than 9 we see that $\phi(9) = 6$.

   We have $5555 \equiv 2 \bmod 9$ and $2222 \equiv -1 \bmod 9$. Thus

$$5555^{2222} + 2222^{5555} \equiv 2^{2222} + (-1)^{5555} \equiv 2^{2222} - 1 \bmod 9,$$

   using 5555 is odd. Euler's Theorem and $2222 = 370 \times 6 + 2$ together give
$$2^{2222} - 1 \equiv \left(2^6\right)^{370} 2^2 - 1 \equiv 2^2 - 1 = 3 \bmod 9.$$

   Hence
$$5555^{2222} + 2222^{5555} \equiv 3 \bmod 9.$$

Thus $5555^{2222}+2222^{5555}$ is of the form $3+9\ell$ for some $\ell \in \mathbb{Z}$. Here $3+9\ell = 3(1+3\ell)$ is a multiple of 3, i.e. divisible by 3, but not by 9.

(iii) First

$$3333^{7777}+7777^{3333} \equiv 33^{7777}+77^{3333} \bmod 100.$$

Euler's Theorem modulo 100 states that if $\gcd(a,100)=1$ then $a^{40} \equiv 1 \bmod 100$ since $\phi(100)=40$. Noting that $7777 = 194 \times 40 + 17$ while $3333 = 83 \times 40 + 13$, gives

$$\begin{aligned} 33^{7777}+77^{3333} &= \left(33^{40}\right)^{194} 33^{17} + \left(77^{40}\right)^{83} 77^{13} \\ &\equiv 33^{17}+77^{13} \bmod 100, \end{aligned}$$

since $(33,100)=(77,100)=1$.

Finally, using the method of successive squaring we get $33^{17} \equiv 73 \bmod 100$ and $77^{13} \equiv 17 \bmod 100$. Hence the last two digits of $3333^{7777}+7777^{3333}$ are 90.

4. i) $7^5 \equiv 11 \bmod 13$ and $7^7 \equiv 6 \bmod 13$.

ii) We notice that $6x \equiv 5 \bmod 13$ is, by part i, the same as $7^7 x \equiv 5 \bmod 13$. Fermat's Little Theorem states that $7^{12} \equiv 1 \bmod 13$. So multiplying our congruence by 7^5 gives

$$7^{12}x \equiv 7^5 \times 5 \equiv 11 \times 5 \bmod 13,$$

i.e. $x \equiv 3 \bmod 13$.

5.

	mod 91
2	2
2^2	4
2^4	16
2^8	74
2^{16}	16
2^{32}	74
2^{64}	16

Note how we are lucky here to get a repeating pattern. Then

$$2^{90} = 2^{64}2^{16}2^{8}2^{2} \equiv 16 \times 16 \times 74 \times 4 \equiv 64 \bmod 91.$$

If 91 *were* a prime then Fermat's Little Theorem gives, since $\gcd(2, 91) = 1$,

$$1 \equiv 2^{91-1} = 2^{90} \equiv 64 \bmod 91.$$

This contradiction means that 91 is not a prime.

6. Follow the hint and count the number of integers $1 \le r \le p^k - 1$ that are **not** coprime with p^k. Such integers are of the form mp where

$$1 \le m \le \frac{p^k - 1}{p} = p^{k-1} - \frac{1}{p}.$$

But m is an integer so, in fact, $1 \le m \le p^{k-1} - 1$. Thus there are $p^{k-1} - 1$ integers **not** coprime to p^k out of a possible total of $p^k - 1$ integers. Hence

$$\phi\left(p^k\right) = \left(p^k - 1\right) - \left(p^{k-1} - 1\right) = p^k - p^{k-1} = p^{k-1}(p-1).$$

7. ★ a)

$$\begin{aligned}
\sigma_1\sigma_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix}, \\
\sigma_2\sigma_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 1 & 6 & 2 \end{pmatrix}, \\
\sigma_3\sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}, \\
\sigma_1^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}, \\
\sigma_3^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 6 & 1 \end{pmatrix}, \\
\sigma_1\sigma_2\sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{pmatrix}.
\end{aligned}$$

$$\begin{aligned}
\tau_1\tau_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 6 & 3 & 5 & 8 & 1 & 9 & 4 \end{pmatrix}, \\
\tau_2\tau_1\tau_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 4 & 5 & 8 & 3 & 1 & 6 & 9 \end{pmatrix}, \\
\tau_1^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 & 8 & 9 \end{pmatrix}.
\end{aligned}$$

b)

$$\begin{aligned}
\sigma_1^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix}, \\
\sigma_2^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 6 & 4 \end{pmatrix}, \\
(\sigma_1\sigma_2)^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}, \\
\sigma_3^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 6 & 1 \end{pmatrix}, \\
\tau_1^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 6 & 8 & 5 & 1 & 4 & 3 \end{pmatrix}, \\
\tau_2^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 8 & 6 & 3 & 9 & 2 & 5 & 4 \end{pmatrix}.
\end{aligned}$$

c)

$$\begin{aligned}
\sigma_2^{-1}\sigma_1^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 6 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix} \\
&= (\sigma_1\sigma_2)^{-1}.
\end{aligned}$$