MATH10101, for supervision in week 12. Primes. Permutations — SOLUTIONS

Q34. (i) Use the table below to sieve the integers up to 200 for primes. How many primes are there between 1 and 200?

($\star$)(ii) You are given that the smallest prime not listed in this table is 211. Use results from the course to prove that the smallest composite number which has no prime factor listed in this table is 211^2.

Q34 - solution. (i) 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 there are 46 primes between 1 and 200.

(ii) We need to prove two satements: (1) 211^2 is a composite number whose prime factors are not in the table; (2) if n is composite and n has no prime factors in the table, then $n \geq 211^2$.

Proof of statement (1): the integer 211^2 is composite as it is a product of two integers greater than 1. We are given that 211 is prime, hence the only prime factor of 211^2 is 211, and 211 is not listed in the table. Hence 211^2 indeed has no prime factors in the table.

Proof of statement (2): let n be composite and without prime factors in our table. By a result from the course, a composite n has a prime factor p such that $p \leq \sqrt{n}$. By assumption, p does not appear in the table. Yet the table contains all primes between 1 and 200, hence $p > 200$. Therefore, what we are given implies that $p \geq 211$. Thus, $\sqrt{n} \geq p \geq 211$ which implies that $n \geq 211^2$.

Q35. This question is inspired by **twin primes** — pairs of primes of the form $(p, p+2)$. It is still not known if there are infinitely many twin primes, although progress towards an answer has been made within the last 5 years. We deal with related but easier questions.

(i) Show that there is only one **prime triplet** of the form $(p, p+2, p+4)$. (*Hint* Look at p modulo 3)

(ii) Let $n \in \mathbb{N}$. Show that the $n-1$ numbers $n!+2$, $n!+3$, $\ldots$, $n!+n$ are all composite. Conclude that there exists a prime p such that the next prime after p is greater than or equal to $p+n$. That is, **gaps between consecutive primes can be arbitrarily large**.

Q35 - solution. (i) Assune that p, $p+2$ and $p+4$ are primes. There are three possible cases:

a) If $p \equiv 0 \mod 3$, then $3 \,|\, p$. The only prime divisible by 3 is 3 itself. Hence the only possibility is $(p, p+2, p+4) = (3, 5, 7)$.
b) If $p \equiv 1 \mod 3$, then $p+2 \equiv 1+2 \equiv 0 \mod 3$, hence $3 \,|\, (p+2)$ and, given that $p > 1$ hence $p+2 > 3$, we conclude that $p+2$ cannot be a pime in this case.
c) If $p \equiv 2 \mod 3$, then similarly we observe that $3 \,|\, (p+4)$ hence $p+4$ is not a prime.

Having considered all cases, we conclude that the only prime triplet is $(3, 5, 7)$.

(ii) If $n = 1$, there are no numbers in the given list, and nothing to prove. We therefore assume that $n > 1$. Observe that $n! = 2 \times 3 \times \cdots \times n$ is divisible by 2, as 2 is a factor in $n!$. Hence $n!+2$ is also divisible by 2, and $n!+2 > 2$, hence $n!+2$ is not a prime. For the same reason $n!+k$, $2 \leq k \leq n$, is divisible by k hence is not prime. All these numbers are greater than 1, so by definition, they are composite.

An informal argument showing that "gaps between consecutive primes can be arbitrarily large" can go as follows. Every composite number sits in a gap between two consecutive primes. The numbers $n!+2$, $\ldots$, $n!+n$ are composite without any intervening primes, hence they all belong to the same gap which must have width at least n; recall that n was an arbitrary positive integer.

Here is a formal and detailed proof that there exists a prime p such that the gap between p and the next prime is at least n. Consider the largest prime p such that $p \leq n!+1$ (it exists since there are primes $\leq n!+1$, for example 2, and there are only finitely many of such primes). If p' is the next prime after p (which exists by Euclid's theorem that there are infinitely many primes), then by the choice of p we have $p' \geq n!+2$. But p' cannot be any of the numbers $n!+2, \ldots, n!+n$ because these numbers are composite, hence $p' \geq n!+n+1$. We conclude that $p'-p \geq (n!+n+1)-(n!+1) = n$.

(⋆)**Q36**. Calculate $\phi(10101)$, explaining the steps. Write down the cardinalities of the sets $\mathbb{Z}_{10101}$ and $\mathbb{Z}^*_{10101}$, briefly stating what you use. Calculate $\phi(10101^2)/\phi(10101)$.

Q36 - solution. In general, $\phi(n)$ can be calculated using the two main facts:

$$\phi(p^k) = p^{k-1}(p-1) \qquad \text{if } p \text{ is prime, } k \in \mathbb{N} \text{ (\textit{proved in class})}$$

and

$$\phi(mn) = \phi(m)\phi(n) \qquad \text{if } m, n \text{ are coprime (multiplicativity of } \phi)$$

We need to know the prime factorisation of 10101:

$$10101 = 13 \times 777 = 3 \times 7 \times 13 \times 37.$$

Since distinct primes are pairwise coprime,

$$\phi(10101) = \phi(3)\phi(7)\phi(13)\phi(37) = (3-1)(7-1)(13-1)(37-1) = 5184.$$

By a basic fact from the course, $|\mathbb{Z}_{10101}| = 10101$. By definition of Euler's phi-function, $|\mathbb{Z}^*_{10101}| = \phi(10101) = 5184$.

To calculate $\phi(10101^2)$, we will derive a general formula for $\phi(n^2)$. Let $n = p_1^{k_1} \dots p_r^{k_r}$ be the prime factorisation of n. Then $n^2 = p_1^{2k_1} \dots p_r^{2k_r}$, therefore

$$\phi(n) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1), \quad \phi(n^2) = \prod_{i=1}^{r} p_i^{2k_i-1}(p_i - 1) = \prod_{i=1}^{r} p_i^{k_i} \times \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1) = n\phi(n).$$

Hence $\phi(10101^2)/\phi(10101) = 10101$.

Q37. Use Fermat's Little Theorem and Euler's Theorem to

(i) show that $5555^{2222} + 2222^{5555}$ is divisible by 7,

(ii) show that $5555^{2222} + 2222^{5555}$ is divisible by 3 but not by 9,

(⋆)(iii) show that $\phi(99) = 60$, then calculate the remainder on division of 101^{999907} by 99.

Q37 - solution. (i) We have $5555 \equiv 4 \mod 7$ (e.g., $5555 = 55 \times 101 \equiv 6 \times 3 \equiv 4 \bmod 7$). Note that 4 is coprime to 7 so, by Fermat's Little Theorem, $4^6 \equiv 1 \mod 7$. But $2222 = 370 \times 6 + 2$. Thus

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

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

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

Hence

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

Alternatively note that $5555+2222 \equiv 0 \bmod 7$ so $5555^{2222}+2222^{5555} \equiv 5555^{2222}+(-5555)^{5555} = 5555^{2222}(1 - 5555^{3333})$. Now, $5555 \equiv 4 \bmod 7$ so $5555^{3333} \equiv 4^{3333} \equiv 2^{6666} = (2^{1111})^6$ which is $1 \bmod 7$ by Fermat's Little Theorem. Hence we obtain, modulo 7, $5555^{2222}(1 - 5555^{3333}) \equiv 5555^{2222}(1 - 1) = 0$.

(ii) We immediately examine $5555^{2222} + 2222^{5555} \mod 9$, **not** mod 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 $a^{\phi(9)} \equiv 1 \mod 9$. By the formula

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

for prime p, or simply by listing the integers less than 9, we see that $\phi(9) = 6$.

We have $5555 \equiv 2 \mod 9$ and $2222 \equiv -1 \mod 9$. (*Recall* from **Q25** that a positive integer is congruent, modulo 9, to the sum of its decimal digits.) Thus

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

using that 5555 is odd. Euler's Theorem and $2222 = 370 \times 6 + 2$ together give

$$2^{2222} - 1 \equiv (2^6)^{370} 2^2 - 1 \equiv 2^2 - 1 = 3 \mod 9.$$

Hence

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

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) Since 9 and 11 are coprime and $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$, $\phi(11) = 10$, we conclude that $\phi(99) = \phi(9)\phi(11) = 60$.

Since 101 is coprime to 99, by Euler's theorem $101^{\phi(99)} = 101^{60} \equiv 1 \mod 99$. Observe that 999900 is divisible by 60; let $999900 = 60k$ where $k \in \mathbb{N}$. Then $101^{999907} = 101^{60k+7} = (101^{60})^k 101^7 \equiv 1^k 2^7 \equiv 128 \equiv 29 \mod 99$. Since the residue 29 is between 0 and 98, 29 is the remainder of 101^{999907} modulo 99.

Q38. Let p be a prime. (i) Prove that if $a^2 \equiv 1$ mod p, then $a \equiv 1$ mod p or $a \equiv -1$ mod p.
Hint $a^2 - 1$ is divisible by p and factors as $(a-1)(a+1)$.

(ii) Deduce that the only *self-inverses* in $\mathbb{Z}_p^*$ are $[1]_p$ and $[-1]_p$.

(iii) Show that in $\mathbb{Z}_p^*$ one has $[1]_p[2]_p \dots [p-1]_p = [-1]_p$.
Hint Pair each element of $\mathbb{Z}_p^*$ with its inverse. Which elements are not paired up?

(iv) Prove *Wilson's Theorem*: $p > 1$ is a prime iff $(p-1)! \equiv -1$ mod p. (If stuck, see PJE §24.2, p.291.)

Q38 - solution. (i) By definition of congruence, $a^2 \equiv 1$ mod p is equivalent to $p \,|\, (a^2 - 1) = (a-1)(a+1)$. By Euclid's property of a prime, this is the same as $(p \,|\, (a-1))$ or $(p \,|\, (a+1))$. By definition of congruence again, this rewrites as $a \equiv 1$ mod p or $a \equiv -1$ mod p.

(ii) A self-inverse is an element $[a]_p$ of $\mathbb{Z}_p$ such that $[a]_p^{-1} = [a]_p$. Equivalently, $[a]_p^2 = [1]_p$. The result of (i) is interpreted, in terms of congruence classes mod p, as the statement $[a]_p^2 = [1]_p \implies [a]_p \in \{[1]_p, [-1]_p\}$. (If $p = 2$, this set consists only of $[1]_2$; otherwise it has two elements.)

(iii) By (ii), the classes $[2]_p, \ldots, [p-2]_p$ are divided into pairs $\{[a]_p, [a]_p^{-1}\}$ (two distinct elements in each pair). The product of each pair is $[1]_p$, hence $[2]_p \ldots [p-2]_p = [1]_p$. It remains to multiply this by $[1]_p$ and by $[p-1]_p = [-1]_p$, obtaining $[-1]_p$.

(iv) If p is a prime, by (iii) $[(p-1)!]_p = [-1]_p$ which reads $(p-1)! \equiv -1 \bmod p$.

Now if $n > 1$ is not prime, then n is composite. Then n has divisor d with $1 < d \leq n-1$. Hence d will be among the factors in $(n-1)!$. This means that $(n-1)!$ and n have a common divisor $d > 1$, hence are not coprime. In particular, $[(n-1)!]_n$ is not invertible in $\mathbb{Z}_n$ so cannot equal $[-1]_n$. We proved that if $n > 1$ is not prime, then $(n-1)! \not\equiv -1 \bmod n$.

(⋆)**Q39**. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} \in S_6$.

(i) Write down the permutations $\sigma\tau$, $\tau\sigma^2$ in two-line notation. Pay attention to the order in which you apply the permutations when multiplying them!

(ii) Find the inverses of σ, τ, $\sigma\tau$.

(iii) Verify that $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$, directly multiplying the permutations on the right-hand side.

Q39 - solution. i)

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix}, \quad \tau\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

ii)

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix}, \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 6 & 4 \end{pmatrix}, (\sigma\tau)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}.$$

iii)

$$\tau^{-1}\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}$$

which coincides with $(\sigma\tau)^{-1}$.