MATH10101, for supervision in week 12. Primes. Permutations

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.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

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**.

($\star$)**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 $\phi(10101^2)/\phi(10101)$.

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,

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

Q38. Let p be a prime. (i) Prove that if $a^2 \equiv 1 \bmod p$, then $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.
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 $[1]_p[2]_p \ldots [p-1]_p = [-1]_p$.
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 $(p-1)! \equiv -1 \bmod p$. (If stuck, see PJE §24.2, p.291.)

($\star$)**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.