Solutions to Exam 18-08-11

Q.1 Corollary 5.5 in the lecture notes.

Q.2 (i) The limsup is 1 and the liminf is zero. To see the former, consider a prime p. One has $\phi(p) = p - 1$ and, since there are infinitely many primes, one has

$$\lim_{p\to\infty} \frac{\phi(p)}{p} = \lim_{p\to\infty} 1 - \frac{1}{p} = 1.$$

To see that the liminf is zero, recall the general formula that

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Hence, it suffices to know that the infinite product on the right, taken over all primes, converges to zero. This follows from Theorem 5.3 in the lecture notes, upon letting $s \to 1^+$.

(ii) One may check by hand that 1237 is a prime, hence the multiplicative group $\mathbb{Z}_{1237}^{\times}$ is cyclic of order 1236. A primitive root is just a generator of this cyclic group, and the number of generators is

$$\phi(1236) = \phi(2^2 \cdot 3 \cdot 103) = (2^2 - 2)(3 - 1)(103 - 1) = 408.$$

(iii) For 3 to be a primitve root means that $3^n \not\equiv 1 \pmod{41}$ for any n which properly divides 40, i.e.: for any $n \in \{1, 2, 4, 5, 8, 10, 20\}$. However, one may directly verify that $3^8 = (3^4)^2 = 81^2 \equiv (-1)^2 \equiv 1 \pmod{41}$. Hence, 3 is not a primitive root modulo 41.

Q.3 Theorem 7.11 in the lecture notes.

Q.4 (i) Since R_n is the least x for which there exist n primes in the interval $(x/2, x]$, it means that there are less than n primes in the interval $(\frac{x-1}{2}, x - 1]$. But in going from here to $(x/2, x]$, the only number we add in is x, and hence this must be a new prime.

(ii) The Prime Number Theorem says that $\pi(x) \sim \frac{x}{\log x}$. This is equivalent to $p_n \sim n \log n$. Hence $p_{2n} \sim 2n \log n$. Now let $N(x)$ denote the number of primes in the interval $(x/2, x]$. Thus

$$N(x) = \pi(x) - \pi(x/2) \sim \frac{x}{\log x} - \frac{x/2}{\log(x/2)} \sim \frac{1}{2}\frac{x}{\log x}.$$

In particular,

$$N(R_n) = n \sim \frac{1}{2}\frac{R_n}{\log R_n},$$

which is equivalent to $R_n \sim 2n \log n \sim p_{2n}$, as desired.

Q.5 (i) Theorem 12.4 in the lecture notes.
(ii) Corollary 12.6 in the lecture notes.

Q.6 I will only sketch the idea, the reader can fill in the rigorous details. Suppose $A = \{a_1 < a_2 < \cdots a_n < \cdots\}$ is an asymptotic basis and the 2-fold representation function is ultimately one. The latter implies, on the one hand, that from some point n_0 on, the consecutive differences

$$a_{n_0+1} - a_{n_0}, a_{n_0+2} - a_{n_0+1}, \cdots$$

must all be distinct. Now the sum of k distinct positive integers is at least $k^2/2 - O(k)$. From this we can deduce that

$$a_n \geq \frac{n^2}{2} - O(n). \tag{1}$$

On the other hand, since A is an asymptotic basis, all but $O(1)$ of the numbers up to a_n can be expressed as sums $a_i + a_j$, for some $1 \leq i, j \leq n$. There are $n^2/2 + O(n)$ such sums, and hence

$$a_n \leq \frac{n^2}{2} + O(n). \tag{2}$$

From (1) and (2) it follows that $a_n = n^2/2 + O(n)$. But this is true for all n, and from it one can easily see that a positive proportion (as $n \to \infty$) of the sums $a_i + a_j$, for $1 \leq i, j \leq n$, must in fact be greater than a_n. This means that (2) can be replaced by $a_n \leq n^2/a + O(n)$, for some $a > 2$. This will then contradict (1), for all $n \gg 0$.

Q.7 (i) $W(k, l)$ is the least positive integer n such that any k-coloring of the set $\{1, 2, ..., n\}$ must yield a monochromatic l-term arithmetic progression.
(ii) See the proofs of equations (22.2) and (22.3) in the lecture notes.

Q.8 Let B (resp. C) denote the subsets of odd (resp. even) elements of A. Let $|A| = n$, $|B| = k$, $|C| = l$, so that $k + l = n$, and denote

$$A = \{a_1 < \cdots < a_n\}, \quad B = \{b_1 < \cdots < b_k\}, \quad C = \{c_1 < \cdots < c_l\}.$$

Now

$$b_1 + 2a_1 < b_1 + 2a_2 < \cdots < b_1 + 2a_n < b_2 + 2a_n < \cdots < b_k + 2a_n$$

is a collection of $n+k-1$ distinct odd elements of $A+2\cdot A$, whereas

$$c_1+2a_1<c_1+2a_2<\cdots<c_1+2a_n<c_2+2a_n<\cdots<c_l+2a_n$$

is a collection of $n+l-1$ distinct even elements of $A+2\cdot A$. Hence, $|A+2\cdot A|\geq(n+k-1)+(n+l-1)=2n+(k+l)-2=3n-2$, as desired.