Solutions to the 2020-03-16 exam

Note. The following solutions do not include all computations. The computations do need to be included on the actual exam.

Question 1

(a) The binary expansion of 840 is $2^3 + 2^6 + 2^8 + 2^9$. By successively squaring the number 93 modulo 197, we find the following table.

n	0	1	2	3	4	5	6	7	8	9
93^{2^n}	93	178	164	104	178	164	104	178	164	104

Hence $93^{840} = 93^{2^3} \cdot 93^{2^6} \cdot 93^{2^8} \cdot 93^{2^9} \equiv_{197} 104 \cdot 104 \cdot 164 \cdot 104 \equiv_{197} 1$.

Note. To simplify the computations, one could also note that 197 is prime and that $840 \equiv_{196} 56$, so that by Fermat's little theorem we have $93^{840} \equiv_{197} 93^{56}$.

(b) Let g be a primitive of $\mathbb{F}_p$. Then $x = g^n$ is a solution to $x^e \equiv_p 1$ if and only if $p - 1$ divides $n \cdot e$. Let n_0 be the smallest n for which this holds. Since the order of g is $p - 1$, we see that $n_0 = \frac{p-1}{\gcd(e,p-1)}$ and that for any solution to $g^{ne} \equiv_p 1$, the number n is divisible by n_0. In particular, the set of solutions modulo p is given by

$$\{g^{k \cdot n_0} \mid 0 \leq k \cdot n_0 < p - 1\}.$$

Since $\frac{p-1}{n_0} = \gcd(e, p - 1)$, we see that $0 \leq k \cdot n_0 < p - 1$ holds if and only if $0 < k < \gcd(e, p - 1)$, hence there are exactly $\gcd(e, p - 1)$ solutions.

(c) Since 2 is a primitive root, it has order 100 in $\mathbb{F}_{101}^*$. Since $32 = 2^5$, we see that 32 has order 20 in $\mathbb{F}_{101}^*$. In particular, if x is a solution to $32^x \equiv_{101} 14$, then all other solutions are of the form $x + 20k$ where $k \in \mathbb{Z}$. By naively computing powers of 32, we find that $32^2 \equiv_{101} 14$, hence the set of integer solutions to $32^x \equiv_{101} 14$ is given by

$$\{2 + 20k \mid k \in \mathbb{Z}\}.$$

Question 2

(a) Let $N = 3233$ and choose $a = 2$ as a potential witness for the Miller-Rabin test. We first compute that $\gcd(a, N) = 1$. By repeatedly dividing $N - 1 = 3232$ by 2, we find that $3232 = 2^5 \cdot 101$. The next step is to compute $2^{101} \equiv_{3233} 2405$. Since this is not congruent to 1 modulo $N = 3233$, we compute the following table by successive squaring.

n	2405^{2^n}
0	2405
1	188
2	3014
3	2699
4	652

Since none of these numbers is congruent to -1 modulo 3233, we conclude that 3233 is a composite number and that $a = 2$ is a Miller-Rabin witness for 3233.

(b) First note that $70 = 2 \cdot 5 \cdot 7$. We compute

$$\begin{aligned} 7^{5\cdot 7} &\equiv_{71} 70, \quad 64^{5\cdot 7} \equiv_{71} 1 \\ 7^{2\cdot 7} &\equiv_{71} 54, \quad 64^{2\cdot 7} \equiv_{71} 54 \\ 7^{2\cdot 5} &\equiv_{71} 45, \quad 64^{2\cdot 5} \equiv_{71} 45. \end{aligned}$$

By the Pohlig-Hellman algorithm, in order to solve the DLP $7^x \equiv_{71} 64$, we should solve the following three DLPs:

$$\begin{aligned} 70^{x_2} &\equiv_{71} 1 \\ 54^{x_5} &\equiv_{71} 54 \\ 45^{x_7} &\equiv_{71} 45. \end{aligned}$$

As can be read off directly from these congruences, this yields $x_2 = 0$, $x_5 = 1$ and $x_7 = 1$. It therefore remains to solve the following system of congruences

$$\begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv 1 \pmod{5}, \\ x \equiv 1 \pmod{7}. \end{cases}$$

An application of the Chinese remainder theorem yields the solution $x = 36$.

Question 3

(a) Since $P \neq Q$, we first compute $\lambda = \frac{\Delta y}{\Delta x} = \frac{9-2}{7-8} = 6$ in $\mathbb{F}_{13}$. Then $P + Q$ is given by

$$P + Q = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1) = (8, 11).$$

(b) First let us find a random point on E. Clearly, $(0, 1)$ lies on E over $\mathbb{F}_{211}$. Since this this elliptic curve has 202 points, we see that the order of $(0, 1)$ is a divisor of

202, so this point either has order 1, 2, 101 or 202. Since $(0,1) \neq \mathcal{O}$ and since the y-coordinate of this point is nonzero, we see that it can't have order 1 or 2. This means that it either has order 101 or order 202. In either of these cases it follows that the point $(0,1) + (0,1) = (9,183)$ has order 101.

(c) In Lenstra's factorization algorithm, one computes $n!P$ for increasing values of n, and the algorithm finishes either when the computation of $n!P$ fails or when it becomes equal to $\mathcal{O}$. In case that the computation "fails", then this yields a number k such that $1 < \gcd(k, N) < N$, hence one has found a non-trivial factor of N. In the case that $n!P$ becomes equal to $\mathcal{O}$, then the algorithm finishes without giving a non-trivial factor of N. By the Chinese remainder theorem, the addition of two points P and Q on E modulo $N = pq$ fails precisely if $P + Q = \mathcal{O}$ over $\mathbb{F}_p$ and $P + Q \neq \mathcal{O}$ over $\mathbb{F}_q$, or the other way around. In particular, the computation of $n!P$ on E modulo N fails if the order of P on $E(\mathbb{F}_p)$ divides $n!$, while the order of P on $E(\mathbb{F}_q)$ does not divide $n!$, or the other way around.

This means that in order to solve this exercise, we should check for which values of n the numbers 154, 410, 162, 405, 130 and 435 divide $n!$. One can compute that none of these numbers divides 8!, while 162 and 405 divide 9!. This implies that Lenstra's algorithm finishes first for the elliptic curve given by (A_2, a_2, b_2), however that it does not give a non-trivial factor of N. Continuing these computations, one notices that 154, 410, 130 and 435 do not divide 10!, but that 154 divides 11! while none of these other numbers do. This implies that the elliptic curve corresponding to (A_1, a_1, b_1) is the first one for which Lenstra's algorithm finishes and gives you a non-trivial factor.

Question 4

Write $x_i = g^{\alpha_i} h^{\beta_i}$ and $y_i = g^{\gamma_i} h^{\delta_i}$. Iteratively computing $f(x_i)$ and $f(f(y_i))$ produces the table

i	x_i	y_i	α_i	β_i	γ_i	δ_i
0	1	1	0	0	0	0
1	5	25	1	0	2	0
2	25	30	2	0	4	2
3	20	34	2	1	4	4
4	30	25	4	2	5	5
5	24	30	4	3	10	12
6	34	34	4	4	10	14.

We find the collision $x_6 = y_6 = 34$, which yields the congruence $g^4 h^4 \equiv_{37} g^{10} h^{14}$, hence that $g^6 \equiv_{37} h^{-10}$. Using the extended Euclidean algorithm, we find that $\gcd(10, 36) = 2$ and that $25 \cdot -10 \equiv_{36} 2$. In particular, multiplying the exponents on both sides of $g^6 \equiv_{37} h^{-10}$ by 25, we find that

$$g^{6 \cdot 25} \equiv_{37} g^6 \equiv_{37} h^2$$

This means that either $g^3 \equiv_{37} h$ or $g^{21} \equiv_{37} h$. Computing these powers of g, we find that $g^{21} \equiv_{37} 5^{21} \equiv_{37} 23 \equiv_{37} h$ solves the DLP.

Question 5

(a) Note that $N \equiv_{19} 10$ and $N \equiv_{23} 2$.

By definition, $F(a+k)$ is divisible by 19 if and only if $(a+k)^2 \equiv_{19} N \equiv_{19} 10$. By computing squares of integers modulo 19, we find that 10 is not a square modulo 19, hence that there exist no value of $k \geq 0$ such that $F(a+k)$ is divisible by 19

Similarly, $F(a+k)$ is divisible by 23 if and only if $(a+k)^2 \equiv_{23} 2$. By computing squares modulo 23, we find that $5^2 \equiv_{23} 2$, hence that $(a+k)^2 \equiv_{23} 2$ if and only if $a+k \equiv_{23} \pm 5$. Since $a \equiv_{23} 19$, we see that 23 divides $F(a+k)$ if and only if $k \equiv_{23} 9$ or $k \equiv_{23} 22$.

(b) We need to find all products of the 11-smooth numbers

$$\begin{aligned}
(a+1)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7, \\
(a+6)^2 - N &= 3^2 \cdot 5 \cdot 7^3, \\
(a+286)^2 - N &= 3^7 \cdot 5 \cdot 7 \cdot 11, \\
(a+421)^2 - N &= 2^2 \cdot 3^3 \cdot 5 \cdot 7^4, \\
(a+3289)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^3, \\
(a+4389)^2 - N &= 2^2 \cdot 3^2 \cdot 5^7 \cdot 11, \\
(a+5951)^2 - N &= 2^2 \cdot 5^3 \cdot 7 \cdot 11^4,
\end{aligned}$$

that are perfect squares. This amounts to doing linear algebra over $\mathbb{F}_2$ with the exponents of the prime numbers on the right-hand side of the equations above. To this end, consider the matrix

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

where the columns correspond to the 11-smooth numbers given above, and the rows to the prime factors 2, 3, 5, 7 and 11. More precisely, the entry at the i-th row and j-th column is equal to 1 if, for the j-th 11-smooth number given above, the exponent of the i-th prime factor is an odd number, and this entry is equal to 0 otherwise. The perfect squares that can be formed using the given 11-smooth numbers correspond to elements of the kernel of M. Since we are working modulo 2, the number of elements in $\ker(M)$ is equal to $2^{\dim(\ker(M))}$. Performing Gaussian elimination on the matrix M (modulo 2) yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This shows that M has rank 3. Since M has seven columns, it follows that its kernel must have dimension 4, hence that one can form $2^4 = 16$ perfect squares out of the given 11-smooth numbers. Note, however, that this also includes the case $0 = 0^2$, hence there are 15 non-trivial perfect squares that can be formed. Two examples of vectors in the kernel of M are $(0,1,0,0,0,0,1)$ and $(0,1,1,0,1,0,0)$, which correspond to the perfect squares

$$(a+6)^2(a+5951)^2 = 9727416^2 \equiv_N 2^2 \cdot 3^2 \cdot 5^4 \cdot 7^4 \cdot 11^4$$

and

$$(a+6)^2(a+286)^2(a+3289)^2 = 9972310144^2 \equiv_N 2^2 \cdot 3^{10} \cdot 5^4 \cdot 7^6 \cdot 11^4$$

respectively.

(c) The Euclidean algorithm gives us

$$\gcd(9727416 - 2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^2, N) = 1,$$

so the first factor perfect square does not give us a non-trivial factor of N. However,

$$\gcd(9972310144 - 2 \cdot 3^5 \cdot 5^2 \cdot 7^3 \cdot 11^2, N) = 1613,$$

so we have found that 1613 is a non-trivial factor of N.