Solutions to the 2020-04-20 exam

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

Question 1

(a) We first invert the coefficients in front of the variable x. We see that $3 \cdot 5 \equiv_7 1$, that $3 \cdot 7 \equiv_{10} 1$ and that $7 \cdot 4 \equiv_{27} 1$, hence the given system of congruences is equivalent to

$$\begin{cases} x \equiv 5 \cdot 4 \equiv 4 \pmod 7 \\ x \equiv 4 \cdot 7 \equiv 8 \pmod{10} \\ x \equiv 19 \cdot 4 \equiv 22 \pmod{27} \end{cases}$$

The first congruence yields that $x = 7k + 4$ for some $k \in \mathbb{Z}$. Inserting this in the second congruence yields $7k \equiv_{10} 8 - 4 \equiv_{10} 4$. Since 3 is a multiplicative inverse for 7 modulo 10, we find that $k \equiv_{10} 3 \cdot 4 \equiv_{10} 2$. In particular, we find that $x = 7(10l + 2) + 4 = 70l + 18$ for some $l \in \mathbb{Z}$. The third congruence now yields that

$$16l \equiv_{27} 70l \equiv_{27} 22 - 18 \equiv_{27} 4.$$

The extended Euclidean algorithm can be used to compute that 22 is a multiplicative inverse of 16 modulo 27, hence $l \equiv_{27} 22 \cdot 4 \equiv_{27} 7$. We see that the integer solutions to the given system of congruences are given by $x = 70(27m + 7) + 18 = 1890m + 508$ where $m \in \mathbb{Z}$.

(b) First suppose that $g \in G$ is a generator. Then $\operatorname{ord}(g) = N$ by definition, hence $g^{N/p_i} \neq 1$ since $0 < N/p_i < N$. Conversely, suppose that an element $g \in G$ is given such that $g^{N/p_i} \neq 1$ for all prime factors p_i of $N = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k} = |G|$. By Lagrange's Theorem, $\operatorname{ord}(g)$ is a divisor of $N = |G|$. If g is not a generator of G, then $\operatorname{ord}(g) < N$, hence there must be a prime number p_i such that $p_i^{r_i}$ does not divide $\operatorname{ord}(g)$. This implies that $g^{N/p_i} = 1$, which is a contradiction. We therefore conclude that g is a generator of G.

(c) Fix a primitive root g of $\mathbb{F}_p$. Then $a = g^n$ for a unique $0 \leq n < p - 1$. The equation $x^2 \equiv_p a$ has a solution if and only if n is even. Assume this is the case and write $n = 2i$. Then

$$(a^{(p+1)/4})^2 \equiv_p g^{2 \cdot 2i \cdot (p+1)/4} \equiv_p g^{(p+1)i} \equiv_p g^{2i} \equiv_p a,$$

where we use that $p+1 \equiv_{p-1} 2$. This shows that $a^{(p+1)/4}$ and $-a^{(p+1)/4}$ are the two solutions to $x^2 \equiv_p a$. On the other hand, if n is odd, then write $n = 2j+1$. A computation similar to the one above shows that $a^{(p+1)/2} \equiv_p g^{2j+1+(p-1)/2}$. Since $g^{(p-1)/2} \equiv_p -1$, we conclude that $a^{(p+1)/2} = -a$.

Question 2

(a) Let $N = 28409$ and choose $a = 5$ as a potential witness for the Miller-Rabin test. We first compute that $\gcd(a, N) = 1$. By repeatedly dividing $N - 1 = 28408$ by 2, we find that $28408 = 2^3 \cdot 3551$. The next step is to compute that $5^{3551} \equiv_{28409} 1$. Since this is congruent to 1 modulo 28409, the test fails and $a = 5$ is not a witness for the compositeness of 28409.

(b) First note that $221 = 17 \cdot 13$ and that $16 \cdot 12 = 192$. An application of the extended Euclidean algorithm gives us that $\gcd(77, 192) = 1$ and that 5 is a multiplicative inverse of 77 modulo 192. In particular, the congruence

$$x^{77} \equiv_{221} 11$$

has one solution modulo 221, namely $11^5 \equiv_{221} 163$. We conclude that the set of all integer solutions is given by

$$\{77 + 221k \mid k \in \mathbb{Z}\}.$$

(c) First note that 47 is prime, hence the order of 11 divides 46. One can check that $11^2, 11^{23} \not\equiv_{47} 1$, hence the order of 11 must equal 46. Note that $\lfloor\sqrt{46}\rfloor + 1 = 7$. We now make two lists

i	11^i	$41 \cdot 11^{-7i}$
0	1	41
1	11	18
2	27	40
3	15	21
4	24	31
5	29	1
6	37	44
7	31	9

where $11^{-7} \equiv_{47} 44$ is computed by applying the extended Euclidean algorithm to $11^7 \equiv_{47} 31$. We find two collisions, namely $11^0 \equiv_{47} 41 \cdot 11^{-35}$ and $11^7 \equiv_{47} 41 \cdot 11^{28}$. Both of these tell us that $11^{35} \equiv_{47} 41$, so $x = 35$ solves the DLP.

Note. Strictly speaking, we did not have to check whether the order of 11 equals 46 in order to use $\lfloor\sqrt{46}\rfloor + 1 = 47$. As long as $\mathrm{ord}(11) \leq 46$, then we know that Shank's baby-step giant-leap algorithm will always find at least one collision, given that a solution exists.

Question 3

(a) Make the following two tables for $\mathbb{F}_{17}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^3+x+4	4	6	14	0	4	15	5	14	14	11	11	3	10	4	8	11	2

and

y	0	1	2	3	4	5	6	7	8
y^2	0	1	4	9	16	8	2	15	13

By comparing these tables, we find that the set of points on the given elliptic curve over $\mathbb{F}_{17}$ is

$$\{(0,\pm 2),(3,0),(4,\pm 2),(5,\pm 7),(13,\pm 2),(14,\pm 5),(16,\pm 6),\mathcal{O}\}.$$

(b) A point on an elliptic curve has order 2 if and only if its y-coordinate is 0. The polynomial x^3-x has three zeroes over $\mathbb{F}_{37}$, namely $x=0$ and $x=\pm 1$. In particular, the elliptic curve E has three points of order 2, namely $(0,0)$, $(1,0)$ and $(-1,0)$. Since any cyclic group has at most one point of order 2, we conclude that the group of points of E over $\mathbb{F}_{37}$ is not cyclic.

(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 151, 401, 160, 406, 156 and 408 divide $n!$. One can compute that none of these numbers divides $7!$, while 160 divides $8!$. This implies that the elliptic curve corresponding to (A_2,a_2,b_2) is the first one for which Lenstra's algorithm finishes and gives you a non-trivial factor.

Question 4

Throughout this question, Theorem 6.6 of the book is used to compute the sums of points on $E(\mathbb{F}_{107})$. Note that $102=2\cdot 3\cdot 17$. In order apply Pohlig-Hellman, we first to compute $2\cdot 3P=6P$, $2\cdot 17P=34P$ and $3\cdot 17P=51P$. Using the given table, this comes down to computing

$$\begin{aligned}
6P &= 2P+4P=(36,87)+(3,101)=(22,40),\\
34P &= 2P+32P=(36,87)+(51,41)=(47,68),\\
51P &= 34P+16P+P=(47,68)+(28,66)+(4,17)=(106,0).
\end{aligned}$$

Note that since none of these points is $\mathcal{O}$, question 1(b) tells us that the order of P on $E(\mathbb{F}_{107})$ is 102. We now need to compute $6Q$, $34Q$ and $51Q$ as well. In order to compute $6Q$, we first compute $2Q = (47,39) + (47,39) = (47,68)$. Since Q and $2Q$ have the same x-coordinates, we see that they must be inverse to each other; i.e. $Q + 2Q = \mathcal{O}$. In particular, Q has order 3. Since $6 \equiv_3 0$, while $34 \equiv_3 1$ and $51 \equiv_3 0$, we see that

$$\begin{aligned} 6Q &= 0Q = \mathcal{O}, \\ 34Q &= Q = (47,39), \\ 51Q &= 0Q = \mathcal{O}. \end{aligned}$$

We now need to solve the following three elliptic curve DLPs:

$$\begin{aligned} x_{17} \cdot 6P &= x_{17}(22,40) = 6Q = \mathcal{O}, \\ x_3 \cdot 34P &= x_3(47,68) = 34Q = (47,39), \\ x_2 \cdot 51P &= x_2(106,0) = 51Q = \mathcal{O}. \end{aligned}$$

It can be seen directly that $x_{17} = 0$, $x_2 = 0$ and $x_3 = -1$ solve these DLPs. In particular, a solution to the original DLP $xP = Q$ can be found by solving the system of congruences

$$\begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv -1 \pmod{3}, \\ x \equiv 0 \pmod{17}. \end{cases}$$

An application of the Chinese remainder theorem yields that $x = 68$ is a solution.

Question 5

(a) Note that $N \equiv_{19} 5$ and $N \equiv_{23} 18$.

By definition, $F(a+k)$ is divisible by 19 if and only if $(a+k)^2 \equiv_{19} N \equiv_{19} 5$. By computing squares of integers modulo 19, we find that $9^2 \equiv_{19} 5$, hence that $(a+k)^2 \equiv_{19} 5$ if and only if $a+k \equiv_{19} \pm 9$. Since $a \equiv_{19} 14$, we see that 19 divides $F(a+k)$ if and only if $k \equiv_{19} 14$ or $k \equiv_{19} 15$.

Similarly, $F(a+k)$ is divisible by 23 if and only if $(a+k)^2 \equiv_{23} 18$. By computing squares modulo 23, we find that $8^2 \equiv_{23} 18$, hence that $(a+k)^2 \equiv_{23} 18$ if and only if $a+k \equiv_{23} \pm 8$. Since $a \equiv_{23} 7$, we see that 23 divides $F(a+k)$ if and only if $k \equiv_{23} 1$ or $k \equiv_{23} 8$.

(b) We need to find all products of the 13-smooth numbers

$$\begin{aligned} (a+59)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7, \\ (a+154)^2 - N &= 3^2 \cdot 5 \cdot 7^3, \\ (a+559)^2 - N &= 3^7 \cdot 5 \cdot 7 \cdot 11, \\ (a+1168)^2 - N &= 2^2 \cdot 3^3 \cdot 5 \cdot 7^4, \\ (a+2098)^2 - N &= 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^3, \\ (a+2343)^2 - N &= 2^2 \cdot 3^2 \cdot 5^7 \cdot 11, \end{aligned}$$

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

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

where the columns correspond to the 11-smooth numbers given above, and the rows to the prime factors 2, 3, 5, 7, 11 and 13. More precisely, the entry at the i-th row and j-th column is equal to 1 if, for the j-th 13-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 13-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

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

This shows that M has rank 3. Since M has six columns, it follows that its kernel must have dimension 3, hence that one can form $2^3 = 8$ perfect squares out of the given 13-smooth numbers. Note, however, that this also includes the case $0 = 0^2$, hence there are 7 non-trivial perfect squares that can be formed. Two examples of vectors in the kernel of M are $(1, 0, 1, 0, 0, 0)$ and $(0, 1, 0, 0, 1, 0)$, which correspond to the perfect squares

$$(a + 59)^2(a + 559)^2 = 2364864^2 \equiv_N 3^4 \cdot 5^8 \cdot 7^2 \cdot 13^2$$

and

$$(a + 154)^2(a + 2098)^2 = 4695841^2 \equiv_N 2^2 \cdot 3^{14} \cdot 5^2 \cdot 7^2 \cdot 13^2,$$

respectively.

(c) The Euclidean algorithm gives us

$$\gcd(2364864 - 3^2 \cdot 5^4 \cdot 7 \cdot 13, N) = 1181$$

and

$$\gcd(4695841 - 2 \cdot 3^7 \cdot 5 \cdot 7 \cdot 13, N) = 1181,$$

so both perfect squares that we found give us the same factor 1181 of N.