SOLUTIONS TO HOMEWORK 2

1. (i) Use the Euclidean algorithm:

$$\begin{aligned} 3992 &= 2023 \cdot 1 + 1969 \\ 2023 &= 1969 \cdot 1 + 54 \\ 1969 &= 54 \cdot 36 + 25 \\ 54 &= 25 \cdot 2 + 4 \\ 25 &= 4 \cdot 6 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Then identifying the last non-zero remainder, we find that $(3992, 2023) = 1$.
(ii) Now we work backwards.

$$\begin{aligned} 1 &= 25 - 4 \cdot 6 = 25 - (54 - 25 \cdot 2) \cdot 6 = 25 \cdot 13 - 54 \cdot 6 \\ &= (1969 - 54 \cdot 36) \cdot 13 - 54 \cdot 6 = 1969 \cdot 13 - 54 \cdot 474 \\ &= 1969 \cdot 13 - (2023 - 1969) \cdot 474 = 1969 \cdot 487 - 2023 \cdot 474 \\ &= (3992 - 2023) \cdot 487 - 2023 \cdot 474 = 3992 \cdot 487 - 2023 \cdot 961. \end{aligned}$$

Then $1 = 3992 \cdot (487) + 2023 \cdot (-961)$, and so $(x, y) = (487, -961)$ is a solution of the equation $3992x + 2023y = 1$.
(iii) If n is of the form $21x + 39y$, then necessarily $3|n$. We can solve $3m + 91z = 1$ by using the Euclidean algorithm (or directly!): you may check that $3 \cdot (-30) + 91 \cdot 1 = 1$. Now we solve $21x + 39y = 3 \cdot (-30)$. By the Euclidean algorithm (or otherwise!), we may find the solution $(x, y) = (2, -1)$ to the equation $21x + 39y = 3$, and hence $21 \cdot 2 \cdot (-30) + 39 \cdot (-1) \cdot (-30) = 3 \cdot (-30)$. So $21 \cdot (-60) + 39 \cdot 30 + 91 \cdot 1 = 1$, and a suitable solution is $(x, y, z) = (-60, 30, 1)$

2. Since $(a, b) = 111$, one has $111|a$ and $111|b$, say $a = 111A$ and $b = 111B$. Then $(A, B) = 1$ and $[111A, 111B] = 999$, whence $[A, B] = 9$ and $AB = (A, B)[A, B] = 9$. The latter implies that $A|9$ and $B|9$, so that $A, B \in \{1, 3, 9\}$. But $(A, B) = 1$ and $AB = 9$, so $\{A, B\} = \{1, 9\}$. Then (a, b) must be one of $(111, 999)$ and $(999, 111)$, both of which satisfy $(a, b) = 111$ and $[a, b] = 999$.

3. (i) The prime factorisation of a positive integer may be written uniquely in the form $n = \prod_{p|n} p^{r(p)}$, with the $r(p)$ positive integers. By the division algorithm, there are unique integers $c(p)$ and $d(p)$ with $r(p) = 2c(p) + d(p)$ and $d(p) = 0$ or 1, for each p. But then n can be written uniquely in the form $n = ab$, where $b = \left(\prod_{p|n} p^{c(p)}\right)^2$ and $a = \prod_{p|n} p^{d(p)}$. The proof is completed by noting that a is squarefree, for otherwise, if $m^2|a$ with $m > 1$, then $q^2|a$ with q a prime divisor of m, contradicting the prime factorisation of a.
(ii) Suppose that n is a squarefull number, and that for each prime number p dividing n, the largest power of p dividing n is p^{r_p}. Then one has $r_p \geqslant 2$, so

that for some $k_p \in \mathbb{Z}_{\geqslant 0}$, one has $r_p = 6k_p + s_p$ for some $s_p \in \{2, 3, 4, 5, 6, 7\}$. Each element in the latter set may be written in the form $s_p = 2u_p + 3v_p$, with u_p a non-negative integer and $v_p = 0$ or 1. Then

$$n = \prod_{p|n} p^{r_p} = \Big(\prod_{p|n} p^{3k_p+u_p}\Big)^2 \Big(\prod_{p|n} p^{v_p}\Big)^3,$$

and the desired conclusion is now immediate.

4. (i) All primes exceeding 3 have the form $6k+1$ or $6k+5$. Suppose that there are just finitely many prime numbers of the shape $6k+5$. Let the set of all such primes exceeding 3 be $\{p_1, p_2, \ldots, p_n\}$, and put $Q = 6p_1 \ldots p_n - 1$. Plainly, one cannot have $p_i | Q$ for any i with $1 \leqslant i \leqslant n$. Further, neither 2 nor 3 divides Q. If the only primes dividing Q were of the form $6k+1$, then Q would itself be of the form $6k+1$, which is not the case. So Q must have a prime factor of the form $6k+5$ that is not one of $p_1, \ldots, p_n$. This contradicts our assumption that the latter are the only primes of such shape. So there are infinitely many primes not of the shape $6k+5$.
(ii) All primes exceeding 5 have the form $10k \pm a$ with $a = 1$ or 3. Suppose that all large enough primes are of the form $10k \pm 1$, so that there are only finitely many of the form $10k \pm 3$. Let the set of all such primes exceeding 3 be $\{p_1, p_2, \ldots, p_n\}$, and put $Q = 10p_1 \ldots p_n - 3$. Plainly, one cannot have $p_i | Q$ for any i with $1 \leqslant i \leqslant n$. Further, neither 2 nor 5 divides Q. If the only primes dividing Q were of the form $10k \pm 1$, then Q would itself be of the form $10k \pm 1$, which is not the case. So Q must have a prime factor of the form $10k \pm 3$ that is not one of $p_1, \ldots, p_n$. This contradicts our assumption that the latter are the only primes of such shape. So there are infinitely many primes not of the shape $10k \pm 1$, and the answer is "no!".

5* **[Hard].** Write $a_i = (2b_i+1)2^{c_i}$, with $b_i, c_i \in \mathbb{Z}_{\geqslant 0}$, for $1 \leqslant i \leqslant k$. Then $1 \leqslant 2b_i + 1 < 2n$ for each i, and hence $0 \leqslant b_i \leqslant n-1$ for each i. Now if for any $i < j$ we have $b_i = b_j$, then since $a_i < a_j$, we have $c_i < c_j$, and so $a_i | a_j$, which is a contradiction. So $b_i \neq b_j$ for $i \neq j$. Then since there are at most n distinct choices for b_i, there are at most n elements a_i, that is, one has $k \leqslant n$.

Suppose that $k = n$, and that m is the integer satisfying $3^m < 2n < 3^{m+1}$. By the preceeding argument, we see that for each integer j with $0 \leqslant j \leqslant n-1$, there is an i with $b_i = j$. Let d be maximal with $(2b_1+1)3^d < 2n$, and consider the indices $1 < i_1 < i_2 < \cdots < i_d$ with $2b_{i_r} + 1 = 3^{d_{i_r}}(2b_1+1)$, for some integer d_{i_r}. Now, if $c_{i_r} < c_{i_{r+1}}$, then $a_i | a_j$. Then we have $c_1 > c_{i_1} > \cdots > c_{i_d}$, and in particular, $c_1 \geqslant d$. Therefore, since $(2b_1+1)3^{d+1} > 2n$, we have $3^m \leqslant 2n - 1 \leqslant (2b_1+1)3^{d+1} - 1$. So $2b_1 + 1 \geqslant 3^{m-d-1} + 3^{-d-1}$, that is, $2b_1 + 1 \geqslant 3^{m-d-1} + 1$. Now for each positive integer k, one has $3^{k-2} + 1 \geqslant 2^{k-1}$, and so $a_1 = (2b_1+1)2^{c_1} \geqslant 2^{m-d}2^d = 2^m$.