38th VTRMC, 2016, Solutions

1. Write $I = \int_1^2 \frac{\ln x}{2-2x+x^2}\,dx$. We make the substitution $y = 2/x$. Then $dx = -2y^{-2}dy$ and we have
$$I = \int_2^1 \frac{-2y^{-2}\ln(2/y)}{2-4/y-4/y^2}\,dy = \int_1^2 \frac{\ln 2 - \ln y}{y^2-2y+2}\,dy.$$
Therefore
$$2I = \int_1^2 \frac{\ln 2}{y^2-2y+2}\,dy = \int_0^1 \frac{\ln 2}{x^2+1}\,dx$$
by making the substitution $x = y-1$. We conclude that $I = \dfrac{\pi \ln 2}{8}$.

2. Set $a_n = \frac{(2n)!}{4^n n! n!}$. Then $a_n/a_{n-1} = (2n-1)/(2n) = 1 - 1/(2n)$. Therefore
$$(n-1)/n \le (a_n/a_{n-1})^2 \le n/(n+1)$$
for all $n \in \mathbb{N}$. Now if $b_n = 1/n$, then
$$b_n/b_{n-1} \le (a_n/a_{n-1})^2 \le b_{n+1}/b_n.$$
Therefore $1/4n \le a_n^2 \le 1/(n+1)$ and hence
$$\frac{1}{(4n)^{k/2}} \le a_n \le \frac{1}{(n+1)^{k/2}}.$$
Since $\sum 1/n^{k/2}$ is convergent if and only if $k > 2$, we deduce that the series is convergent for $k > 2$ and divergent for $k \le 2$.

3. Let I denote the identity matrix in $\mathrm{M}_n(\mathbb{Z}_2)$. If $A \in \mathrm{M}_n(\mathbb{Z}_2)$ and $A^2 = 0$, then $(I+A)^2 = I + 2A + A^2 = I$ because we are working mod 2, and we see that $I + A \in \mathrm{GL}_n(\mathbb{Z}_2)$, the invertible matrices in $\mathrm{M}_n(\mathbb{Z}_2)$. Conversely if $X \in \mathrm{GL}_n(\mathbb{Z}_2)$, and $X^2 = I$, then $(I+X)^2 = 0$. We deduce that the number of matrices A satisfying $A^2 = 0$ is precisely the number of matrices satisfying $X^2 = I$. Since $n \ge 2$, the number of matrices in $\mathrm{GL}_n(\mathbb{Z}_2)$ is even (if $Y \in \mathrm{GL}_n(\mathbb{Z}_2)$, then we can pair it with the matrix Y' obtained from Y by interchanging the first two rows of Y, and note that $Y \ne Y'$ otherwise Y would have two rows equal and therefore would not be invertible). Now if $Z \in \mathrm{GL}_n(\mathbb{Z}_2)$ and $Z^2 \ne I$, then we can pair it with Z^{-1} and we see that the number of matrices satisfying $Z^2 \ne I$ in $\mathrm{GL}_n(\mathbb{Z}_2)$ is even. Therefore the number of matrices satisfying $X^2 = I$ is even and the result follows.

4. First observe that if $p > 2$ is a prime and $a < p$ is such that a^2+1 is divisible by p, then $a \neq p-a$ and $P(a) = P(p-a) = p$. Indeed a^2+1 and $(p-a)^2+1 = (a^2+1)+p(p-2a)$ are divisible by p and are smaller than p^2, so they cannot be divisible by any prime greater than p.

   We will prove the stronger statement that there are infinitely many primes p for which $P(x) = p$ has at least three positive integer solutions, so assume by way of contradiction that there are finitely many such primes and let s be the maximal prime among these; if there are no solutions, set $s = 2$. Let S be the product of all primes not exceeding s. If $p = P(S)$, then p is coprime to S and thus $p > s$. Let a be the least positive integer such that $a \equiv S \bmod p$. Then a^2+1 is divisible by p, hence $P(a) = P(p-a) = p$ because $p > a$. Let $b = a$ if a is even, otherwise let $b = p-a$. Then $(b+p)^2+1$ is divisible by $2p$, so $P(b+p) \geq p$. If $P(b+p) = p$, we arrive at a contradiction. Therefore $P(b+p) =: q > p$ and $(b+p)^2+1$ is divisible by $2pq$ and thus $(b+p)^2+1 \geq 2pq$. This means $q < b+p$, otherwise $(b+p)^2+1 \leq (2p-1)q+1$ (because $b < p$) $< 2pq$. Now let c be the least positive integer such that $c = b+p \bmod q$. We have $P(c) = P(q-c) = P(b+p) = q > p > s$, another contradiction and the proof is finished.

5. The equality yields $1+m-n\sqrt{3} = (2-\sqrt{3})^{2r-1}$ and hence $(1+m)^2-3n^2 = 1^{2r-1} = -1$. Therefore $m(m+2) = 3n^2$. If $p \neq 2,3$ is a prime and p^a is the largest power of p dividing n, then p^{2a} is the largest power of p dividing $3n^2$. Since p cannot divide both m and $m+2$, we see that either $p \nmid m$ or $p^{2a} \mid m$, in either case the power of p that divides m is an even. It remains to prove that the largest power of 2 and 3 that divides m is also even. Now if 2 divides m, then the largest power of 2 that divides $m(m+2)$, and hence also $3n^2$, is odd which is not possible. All that remains to be proven is that 3 does not divide m. However we have $1+m = 2^{2r-1} \bmod 3$, which shows that 3 does not divide m as required.

6. Write $M = \begin{pmatrix} I+A & -X \\ -Y & I+P \end{pmatrix}, N = \begin{pmatrix} I+B & X \\ Y & I+Q \end{pmatrix}$.

   Then
   $$MN = \begin{pmatrix} I+A+B+AB-XY & AX-XQ \\ PY-YB & I+P+Q+PQ-YX \end{pmatrix} = I.$$

   Therefore $NM = I$ and in particular $I+A+B+BA-XY = I$. The result follows.

7. Proceed by induction on k. Let c_k denote the constant term of f_k. For the base case $k=1$, we need only observe that $f_1(X) = (1-X)(1-qX^{-1}) = 1+q-X-qX^{-1}$ and $c_1 = (1-q^2)/(1-q) = 1+q$. For any k, we have

$$c_{k+1} = \frac{(1-q^{2k+1})(1-q^{2k+2})}{(1-q^{k+1})^2} c_k = \frac{(1-q^{2k+1})(1+q^{k+1})}{1-q^{k+1}} c_k.$$

We will prove that the constant term of $f_k(X)$ satisfies the same recurrence relation, which gives the induction step. Let $a_k^{(i)}$ denote the coefficient of X^i in f_k. From

$$\begin{aligned} f_{k+1}(X) &= (1-q^k X)(1-q^{k+1}X^{-1}) f_k(X) \\ &= (1-q^k X - q^{k+1}X^{-1} + q^{2k+1}) f_k(X) \end{aligned}$$

we deduce that

$$a_{k+1}^{(0)} = (1+q^{2k+1}) a_k^{(0)} - q^k a_k^{(-1)} - q^{k+1} a_k^{(1)}.$$

We want a recurrence relation for $a_k^{(0)}$. To relate $a_k^{(\pm 1)}$ to $a_k^{(0)}$, we consider

$$\begin{aligned} f_k(qX) &= \prod_{i=0}^{k-1} \Big((1-q^{i+1}X)(1-q^i X^{-1}) \Big) \\ &= \frac{(1-q^k X)(1-X^{-1})}{(1-X)(1-q^k X^{-1})} f_k(X) \\ &= \frac{1-q^k X}{q^k - X} f_k(X). \end{aligned}$$

Hence $(q^k - X) f_k(qX) = (1-q^k X) f_k(X)$. Equating coefficients of X^0 and X^1 on both sides, we obtain

$$a_k^{(-1)} = q \frac{q^k-1}{1-q^{k+1}} a_k^{(0)}, \qquad a_k^{(1)} = \frac{q^k-1}{1-q^{k+1}} a_k^{(0)}.$$

Therefore

$$a_{k+1}^{(0)} = \left(1 + q^{2k+1} - 2q^{k+1} \frac{q^k-1}{1-q^{k+1}}\right) a_k^{(0)} = \frac{(1-q^{2k+1})(1+q^{k+1})}{1-q^{k+1}} a_k^{(0)}$$

and this completes the proof.