1. (20 pts) Use mathematical induction to prove the identity

$$(1+\frac{1}{2})(1+\frac{1}{3})\cdots(1+\frac{1}{n}) = \frac{n+1}{2}$$

for all integers $n \geq 2$.

Basis step: for $n=2$, both sides are equal to $3/2$.

Induction step: for $n>2$, assume by induction that

$$(1+\tfrac{1}{2})(1+\tfrac{1}{3})\cdots(1+\tfrac{1}{n-1}) = \frac{n}{2}.$$

Multiply both sides by $(1+\frac{1}{n})$ to get

$$(1+\tfrac{1}{2})(1+\tfrac{1}{3})\cdots(1+\tfrac{1}{n}) = \frac{n}{2}(1+\tfrac{1}{n})$$

$$= \frac{n}{2}\left(\frac{n+1}{n}\right) = \frac{n+1}{2}.$$

2. (20 pts) Find the largest integer n such that n^2 divides 10!. Justify your answer.

The prime factorization of $10! = (2\cdot 5)(3\cdot 3)(2^3)\cdot 7\cdot(2\cdot 3)\cdot 5\cdot(2^2)\cdot 3\cdot 2\cdot 1$ is $2^8\cdot 3^4\cdot 5^2\cdot 7$. Therefore the prime factorization of the largest n such that $n^2 \mid 10!$ is $n = 2^4\cdot 3^2\cdot 5 = 720$.

3. Consider the RSA cryptographic system with modulus $n = 9797 = 97\cdot 101$, and private encryption key $e = 17$, so $E(x) = x^{17} \mod 9797$ is the encryption function. Let d denote the private decryption key, for which $D(x) = x^d \mod 9797$ is the decryption function.

(a) (10 pts) Specify the congruence $Ad \equiv B \pmod{C}$ which d should satisfy.

$17d \equiv 1 \pmod{9600}$.

I.e., d is an inverse of $e \pmod{(p-1)(q-1)}$, where $n = pq$. Here $p = 97$, $q = 101$.

(b) (10 pts) Given the information that $3953\cdot 17 - 7\cdot 9600 = 1$, find d.

This information tells us that $3953\cdot 17 \equiv 1 \pmod{9600}$. Hence $d = 3953$.

4. What can be concluded about whether 949 is prime or composite from:

(a) (10 pts) the information

$$3^{948} \equiv 1 \pmod{949}?$$

This says 949 passes the Fermat test to base 3, but nothing can be concluded from this as to whether 949 is prime or composite.

(b) (10 pts) the information

$$3^{237} \equiv 703 \pmod{949}, \quad 3^{474} \equiv 729 \pmod{949}, \quad 3^{948} \equiv 1 \pmod{949}?$$

Since $729 \not\equiv \pm 1 \pmod{949}$, this shows that 949 fails the Miller test, and is therefore composite. In fact, $949 = 13 \cdot 73$.

5. (20 pts) Find the number of 5-card poker hands containing 3 of a kind (3 cards of the same face value) but nothing better—not 4 of a kind or full house (3 of a kind plus a pair). Express your answer in terms of permutation and combination numbers $P(n,k)$ and $C(n,k)$, powers and products. Do not simplify. Your reasoning should be visible from the form of your answer.

$13 \cdot C(12,2) \cdot C(4,3) \cdot 4^2$

face value for the 3 of a kind

face values for the other two cards

suits for the 3 of a kind

suits for the other two cards.

You could put 4 instead of $C(4,3)$ since the suits for the 3 of a kind could be chosen by picking the missing suit.