Theorems in Modular Arithmetic

Theorem 1 *(remainder cancellation).*
Let m and b be coprime. Then $ma_1 \equiv_b ma_2 \Leftrightarrow a_1 \equiv_b a_2$.
2. Let m is not divisible by the prime p. Prove that
a) Remainders of the integers m, $2m$, $3m$, …, $(p–1)m$ modulo p are distinct.
b) Remainders of $(p–1)!$ and $m^{p-1}(p–1)!$ modulo p are the same.
c) *(Fermat's little theorem).* $p|m^{p-1}-1$
3. Let n be a positive integer not divisible by 17. Show that either $17|n^8+1$, or $17|n^8-1$.
4. Find the remainder of 50^{10000} (mod 101)
5. Prove that for every prime $p>5$ the integer 11...1 ($p-1$ digits) is divisible by p.
6. For a prime p prove that $(a+b)^p \equiv_p a^p+b^p$ for any integers a and b.
7 a) (*Divisibility lemma*). Let m be an integer not divisible by the prime p. Prove that there is exactly one $n \in \{1,2,\ldots,p-1\}$ such that $mn \equiv_p 1$.
b) Prove that for every prime $p>2$ there are exactly two integers among 1, 2, …, p–1 which squares are 1 modulo p.
c) (*Wilson's theorem***)** Prove that $p|(p-1)!+1$ iff p is prime or p=1.

Chinese remainder theorem

Given n pairwise coprime positive integers $m_1, m_2, \ldots, m_n$ and n integers $r_1, r_2, \ldots, r_n$ so that $0 \le r_i < m_i$ for each i = 1, 2, …, n. Let us call $r_1, r_2, \ldots, r_n$ *a set of remainders*, and denote $M=m_1m_2\ldots m_n$

Theorem 8. There is exactly one N so that $0 \le N \le M-1$ and $N \equiv r_i \pmod{m_i}$ for each i = 1, 2, …, n.

8.**1.** There are exactly M different sets of remainders.
8.**2.** Each integer has the set of remainders.
8.**3.** If two integers A and B has the same set of remainders, then $M|A\text{-}B$.

9. Find the minimal positive integer N so that $N \equiv_{32} 25$ and $N \equiv_{25} 32$
10. Prove that for any coprime positive integers $m_1, m_2, \ldots, m_n$ and any remainder set there is integer a so that $a+1 \equiv r_1 (mod\ m_1), a+2 \equiv r_2 (mod\ m_2), \ldots, a+n \equiv r_n (mod\ m_n)$

Credit problems

MT1. Prove that for any positive integer n there exists n consequtive integers so that each of them is divisible by a perfect square greater then 1.
MT2. For any prime $p>5$ prove that $6(p-4)! \equiv_p 1$
MT3 Prove that
a) If a prime $p \equiv_4 3$, then the equation $x^2=-1$ has no solution modulo p.
b) If $p|n^2+1$ for an integer n, then $p \equiv_4 1$
c) there are infinitely many primes $p \equiv_4 1$
MT4. Given $P(x) \in \mathbb{Z}[x]$ Let $N_P(m) = |\{i : 0 \le i \le m-1, P(i) \vdots m\}|$. Prove that if k and m are coprime then $N_P(km) = N_P(k) N_p(m)$.
MT5. Let p and q be coprime positive integers. Prove that $\sum_{k=0}^{pq-1} (-1)^{[\frac{k}{p}]+[\frac{k}{q}]} = 0$ when pq is even and = 1 when pq is odd.

www.ashap.info/Uroki/eng/NYUAD18/index.html