Lec 10

Review

Euclidean algorithm

Find the GCD of 286 and 503.

$$
\begin{array}{lll}
\gcd(503,286) & 503 = 1 \cdot 286 + 217 & 1 = 10 - 1 \cdot 9 \\
= \gcd(286,217) & 286 = 1 \cdot 217 + 69 & 1 = 7 \cdot 10 - 1 \cdot 69 \\
= \gcd(217,69) & 217 = 3 \cdot 69 + 10 & 1 = 7 \cdot 217 - 22 \cdot 69 \\
= \gcd(69,10) & 69 = 6 \cdot 10 + 9 & 1 = 29 \cdot 217 - 22 \cdot 286 \\
= \gcd(10,9) & 10 = 1 \cdot 9 + 1 & 1 = 29 \cdot 503 - 51 \cdot 286 \\
= 1 & 9 = 9 \cdot 1 &
\end{array}
$$

solve linear congruence $ax \equiv b(mod\ m)$ $(gcd(a,m)=1)$

Euler's Theorem / Fermart's Little Theorem

$$
X^{\phi(n)} \equiv 1\ mod\ n\ if\ gcd(x,n)=1 \\
X^{p-1} \equiv 1\ mod\ p\ if\ X \not\equiv\ mod\ p
$$

RSA

$$
p, q, n = pq \\
\phi(n) = (p-1)(q-1) \\
public\ key : (e, n) \\
primite\ key : d \\
gcd(e, \phi(n)) = 1 \\
ed \equiv 1\ mod\ \phi(n)
$$

加、解密过程：

$$
Encryption : M^e\ mod\ n = C \\
Decryption : C^d\ mod\ n = M
$$

Proof

Q : Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \text{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

Case I: $\gcd(M, n) = 1$

$$\begin{aligned} C^{d'} \bmod n &= M^{ed'} \bmod n = M^{k\lambda(n)+1} \bmod n \\ &= (M^{k\lambda(n)} \bmod n) M \bmod n \\ &= \left(M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod n\right)^k M \bmod n \end{aligned}$$

By Fermat's theorem, $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod p = \left(M^{(q-1)/\gcd(p-1,q-1)}\right)^{p-1} \bmod p = 1$ and $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod q = 1$. Then by Chinese Remainder Theorem, we have $C^{d'} \bmod n = M$.

Case II: $\gcd(M, n) = p$

$M = tp$ for some integer $0 < t < q$. We have $\gcd(M, q) = 1$ and $ed' = k\lambda(n) + 1$ for some integer k. By Fermat's theorem, we have

$(M^{k\lambda(n)} - 1) \bmod q = (M^{k(p-1)(q-1)/\gcd(p-1,q-1)} - 1) \bmod q = 0.$

Then

$$\begin{aligned} (M^{ed'} - M) \bmod n &= M(M^{ed'-1} - 1) \bmod n \\ &= tp(M^{k\lambda(n)} - 1) \bmod pq \\ &= 0 \end{aligned}$$

Case III: $\gcd(M, n) = q$

Similar to Case II.

Case IV: $\gcd(M, n) = pq$

Trivial.

Mathematical Induction

Proof by smallest counterexample

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

  - ◇ Suppose that $(*)$ is not always true
  - ◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n
  - ◇ For any nonnegative integer $i < n$,

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

  - ◇ Since $0 = 0 \cdot 1/2$, $(*)$ holds for $n = 0$
  - ◇ The smallest counterexample n is larger than 0

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n - 1$

  - ◇ Substituting $n - 1$ for i gives

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

  - ◇ Adding n to both sides gives

$$(*) \quad 1 + 2 + \cdots + n - 1 + n = \frac{(n-1)n}{2} + n = \frac{n(n+1)}{2}$$

  - ◇ Thus, n is not a counterexample. Contradiction!

Steps:

Example 2

- Let $P(n) - 2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

  ◇ This contradicts $(*)$.

  ◇ Thus, $P(n)$ is true for all $n \in N$.

The week Principle of Mathematical Induction

验证开头正确性，之后假设n正确，去推导n+1的正确性，最后得出结论

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n) - 2^{n+1} \geq n^2 + 3$ Base Step

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3 - P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \quad (*)$

  Inductive Hypothesis

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 6 \\
&= n^2 + 3 + n^2 - 4n + 4 + 1 \\
&= n^2 + 3 + (n-2)^2 + 1 \\
&> n^2 + 3
\end{aligned}
$$

  Inductive Step

  Hence, we've just prove that for $n > 2$, $P(n-1) \rightarrow P(n)$.

  By mathematical induction, $\forall n > 2,\ 2^{n+1} \geq n^2 + 3$.

  Inductive Conclusion

The Strong Principle of Mathematical Induction

Example:

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  $P(1) \wedge \cdots \wedge P(n-1)$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

  ◇ Then, if n is not a prime power, it is a product of two smaller numbers, each of which is, by the inductive hypothesis, a power of a prime or a product of powers of primes.

  ◇ Thus, by the strong principle of mathematical induction, every positive integer is a power of a prime or a product of powers of primes.

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step
  2. We then, $\forall n > b$, show either

     $(*) \qquad P(n-1) \rightarrow P(n)$

     or

     $(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$

     We need to make the inductive hypothesis of either $P(n-1)$ or $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1)$.We then use $(*)$ or $(**)$ to derive $P(n)$.
  3. We conclude on the basis of the principle of mathematical induction that $P(n)$ is true for all $n \geq b$.

Recursion