e. Other name: totient $\phi(n)$ [cardinality of reduced set of residues]
f. Values: $\phi(p) = p - 1$ [as 0x mod n = 1 has no solution]
g. Values: show with 3 and 5; 3 and 7; conclude $\phi(pq) = (p–1)(q–1)$;

Outline for April 7, 1997

1. Greetings and Felicitations
   a. Please speak into the microphone
2. Equivocation
   a. Given some info, how much uncertainty is left
   b. Ex: 8 bit integer, => H(X) = 8; parity bit 0 => H(X|Y) = 7 (work it out)
   c. $H(X|Y) = -\Sigma_{x,y} p(X,Y) \lg(p(X|Y))$
   d. As $p(X,Y) = p(X|Y)p(Y)$, $H(X|Y) = -\Sigma_y p(Y) \Sigma_x p(X|Y) \lg(p(X|Y))$ [joint probability]
3. More examples
   a. Throw die, flip coin; $p(X=3, Y=H) = 1/12 = p(X=3)p(Y=H)$ [independence]
   b. Toss coin; if heads, 3-sided die; if tails, 6-sided die. Prob. result is 3?
      $p(Y=H, X=3) = p(X=3|Y=H)p(Y=H)$ etc.
   c. like b, but prob. result is 4:
      $p(Y=H, X=4) = p(X=4|Y=H)p(Y=H)$ etc.
4. Uncertainty in above
   a. $H(X|Y) = \lg 6 = H(X)$ [independence; as $p(X|Y) = p(X)$ and $\Sigma_y p(Y) = 1$]
   b. $H(X|Y) = (1/2)[\lg 3 + \lg 6] = (1/2) \lg 18$
5. Perfect Secrecy
   a. $H(M|C) = H(M)$ or $p(M|C) = p(M)$
   b. $H(C|M) = H(C)$ or $p(C|M) = p(C)$ [same thing]
6. Unicity distance
   a. given C, what is uncertainty in K?
   b. KHOOR ZRUOG; unicity distance is 0 (k = 23)
   c. J; uncity distance is 1 as it's K=25 (I) or K=9 (A)
   d. Smallest N for which $H(K|C) \approx 0$ is amount of ciphertext needed to uniquely determine key
   e. "unconditionally secure" if no such N exists
   f. Can show: $N = H(K)/D$ => $H(K) - DN = 0$
   g. if number of keys = number of meaningful messages, $H(K) = RN$, so
      $H(K) - DN = RN - DN = (R - D) N = rN \neq 0$
7. Random cipher
   a. For a given K, C, $D_K(C)$ equally likey to produce any (meaningless or meaningful) message
8. Number Theory
   a. Review mod notation, note difference between ours and mathematicians
   b. cite residue (equivalence) classes
   c. show complete set of residues
   d. give principle of modular arithmetic
   e. do 7^{20} mod 9 quickly
9. Inverses and All That
   a. find x s.t. ax mod n = 1
   b. use 2x mod 5 = 1 and 2x mod 4 = 1; point is a relatively prime to x
   c. show output of 2x mod 5 for x = 0, …, 4; then for 2x mod 4
   d. for which a does ax mod n = 1 have a solution? "reduced set of residues"