ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
การสอบกลางภาค ภาคการศึกษาที่ 1 ปีการศึกษา 2560

CPE 121 Discrete Mathematics for Computer Engineering / **CPE (AB)**

วันที่สอบ: 28 กันยายน 2560 **เวลา: 13:00 – 16:00**

คำสั่ง:

1. ไม่อนุญาตให้ใช้เครื่องคิดเลขในห้องสอบ
2. ไม่อนุญาตให้นำเอาเอกสารใดๆ เข้าห้องสอบ
3. ห้ามนำข้อสอบและกระดาษคำตอบออกจากห้องสอบ
4. เขียนชื่อ-นามสกุล รหัสนักศึกษา และเลขที่นั่งสอบในข้อสอบและกระดาษคำตอบทุกหน้า
5. ข้อสอบนี้ประกอบไปด้วย 2 ส่วน: ส่วนที่ 1 มี 20 ข้อ 7 หน้า (20 คะแนน) ส่วนที่ 2 มี 2 ข้อ 2 หน้า (10 คะแนน) และสูตร 1 หน้า รวม 10 หน้า
6. อ่านคำสั่งในแต่ละส่วนอย่างละเอียดก่อนลงมือทำ
7. หากมีข้อสงสัยในข้อสอบ ให้นำเอาข้อสงสัยไปถามอาจารย์ผู้สอนในภายหลัง

ส่วนที่ 1 (20 คะแนน)

คำสั่ง: อ่านคำถามโดยละเอียด และเขียนคำตอบพร้อมคำอธิบายลงในบริเวณคำตอบ

ถ้าให้ p, q และ r เป็น proposition

p: คุณได้คะแนนดีจากการสอบกลางภาค

q: คุณทำแบบฝึกหัดในหนังสือทุกข้อ

r: คุณได้ A ในวิชานี้

ในข้อ 1-2 เขียน Proposition ต่อไปนี้ โดยใช้ p, q และ r และ Operator ทาง Logic ต่างๆ

1. คุณได้ A ในวิชานี้ แต่คุณไม่ได้ทำแบบฝึกหัดในหนังสือทุกข้อ

2. เพื่อที่จะให้ได้ A ในวิชานี้ คุณจำเป็นที่จะต้องได้คะแนนดีจากการสอบกลางภาค

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

3. เขียน Truth Table ของ $(p \rightarrow q) \vee \neg r$

4. จงแสดงให้เห็นว่า System Specification นี้ Consistent หรือไม่
   - เมื่อระบบกำลังถูก upgrade ผู้เข้าจะเข้า file system ไม่ได้
   - ถ้าผู้ใช้เข้า file system ได้ ผู้ใช้จะ save file ได้
   - ถ้าผู้ใช้ save file ไม่ได้ ระบบไม่ได้กำลังถูก upgrade

5. จงพิสูจน์ว่า $\forall x P(x) \vee \forall x Q(x)$ ไม่ได้ Equivalent กับ $\forall x\big(P(x) \vee Q(x)\big)$

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

6. จงใช้กฎของการ Inference พิสูจน์ Premise และข้อสรุปต่อไปนี้
   บางคนในห้องนี้เคยไปอังกฤษ คนที่ไปอังกฤษทุกคนต้องขอ visa ดังนั้นบางคนในห้องนี้เคยขอ visa

7. จงพิสูจน์โดยใช้วิธี contraposition ของ
   If $x + y \geq 2$ then $x \geq 1$ or $y \geq 1$

8. ให้ A = {a, b, c, d} และ B = {1, 2} จงหา $B \times A$

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

9. ถ้า A – B = B – A เมื่อ A และ B เป็นเซ็ตใดๆ จงอธิบายลักษณะของเซ็ต A และ B จากความสัมพันธ์ดังกล่าว

10. จงหา a_0 ถึง a_5 ของ recurrence relation $a_n = 6a_{n-1}$, $a_0 = 2$

11. จงยกตัวอย่างฟังก์ชันทางคณิตศาสตร์ที่เป็น one-to-one แต่ไม่ onto

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

12. กำหนดให้

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

จงหาค่า $A^{[3]}$

13. จงเขียน Pseudocode ของ Algorithm ที่หาผลรวมของ list ของตัวเลข integer

14. จงหา Big-O ของจำนวนการบวกหรือการคูณ ที่ใช้ใน Algorithm นี้

```
t = 0
for i = 1 to 3
     for j = 1 to 4
          t = t + ij
```

15. จงหาตัวเลขจำนวนเต็มมา 3 ตัวที่เป็น 5 modulo 17

16. จงแปลงตัวเลขฐานแปดต่อไปนี้เป็นตัวเลขฐานสิบหก (2017)

17. จงหา Greatest Common Divisor (หรม) ระหว่าง 14039 กับ 1529

18. เลข ISBN-10 ของหนังสือ Elementary Number Theory and Its Applications คือ 0-321-500Q1-8 จงหาว่าตัวเลข Q คืออะไร

19. จงถอดรหัสของ Shift Cipher ที่มี k = -3 และข้อความที่ถูกเข้ารหัสลับแล้วคือ YBPQLCIRZH

20. จงอธิบายบทบาทของ Private Key และ Public Key ใน Public Key Cryptography

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

ส่วนที่ 2 (10 คะแนน)

21. *(5 คะแนน)* จงหาค่า inverse ของ 34 modulo 89

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

22. *(5 คะแนน)* ถอดรหัสลับ (decrypt) ของ EABW EFRO ATMR ASIN ซึ่งมาจากการเข้ารหัสด้วย Block Cipher ขนาด 4 ซึ่งมี $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.

ชื่อ-นามสกุล_____ รหัส_____ เลขที่นั่ง _____

Rule of Inferences

Name	Rule
Modus Ponens	$p \to q$ $\underline{\quad p \quad}$ $\therefore q$
Modus Tollens	$p \to q$ $\underline{\quad \neg q \quad}$ $\therefore \neg p$
Hypothetical Syllogism	$p \to q$ $\underline{p \to r}$ $\therefore p \to r$
Disjunctive Syllogism	$p \vee q$ $\underline{\quad \neg p \quad}$ $\therefore q$
Addition	$\underline{\quad p \quad}$ $\therefore p \vee q$
Simplification	$\underline{p \wedge q}$ $\therefore q$
Conjunction	p $\underline{\quad q \quad}$ $\therefore p \wedge q$
Resolution	$\neg p \vee r$ $\underline{p \vee q}$ $\therefore q \vee r$